Configuring IP Multicasting and Multimedia Services

BayRS Version 13.20
Site Manager Software Version 7.20

BCC Version 4.20

Part No. 117355-D Rev 00
April 1999

NORTEL NETWORKS™

Bay Networks, Inc.
4401 Great America Parkway
Santa Clara, CA 95054

Copyright © 1999 Bay Networks, Inc.

All rights reserved. Printed in the USA. April 1999.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

Bay Networks is a registered trademark and BayRS and BCC are trademarks of Bay Networks, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin xix
Text Conventions xx
Acronyms xxi
Related Publications xxiii
How to Get Help xxiv

Chapter 1
Multicasting and Multimedia Overview

Multicast Host Groups 1-2
Multicast Addresses 1-3
Internet Group Management Protocol 1-3
Distance Vector Multicast Routing Protocol 1-3
Multicasting Extensions to OSPF 1-4
Protocol Independent Multicast 1-4
Resource Reservation Protocol 1-4
Bay Networks Resource Manager 1-5
IGMP Relay 1-5
Multicast Table Manager 1-5
Multicast Migration 1-6
Configuring Multicast Migration 1-12
Using BCC show Commands to View Statistics 1-13

Chapter 2
Starting Multicasting and Multimedia Services

Starting IGMP 2-2
Starting DVMRP 2-4
Starting MOSPF 2-6

Starting PIM 2-7
Configuration Prerequisites 2-7
Starting PIM on the Router 2-8
Starting RSVP 2-10

Chapter 3
Configuring and Customizing IGMP

IGMP Concepts and Terminology 3-2
IGMP Queries 3-2
IGMP Host Reports 3-3
Host Leave Messages 3-3
Customizing IGMP Globally 3-4
Enabling and Disabling IGMP Globally 3-5
Estimating the Number of Groups 3-6
Specifying a Version Threshold Time 3-8
Logging IGMP Messages 3-10
Enabling Join Acknowledgments 3-12
Specifying a Forwarding Cache Limit 3-13
Accepting a Nonlocal Report 3-14
Customizing IGMP on an Interface 3-15
Enabling and Disabling IGMP on an Interface 3-16
Specifying Query Suppression 3-17
Specifying a Query Rate 3-19
Specifying a Membership Timeout Interval 3-21
Specifying a Designated Router Timeout Interval 3-22
Specifying a Maximum Host Response Time 3-24
Specifying the Lifetime of an Mtrace Cache Entry 3-26
Specifying the Static Forward Cache Lifetime 3-27
Configuring a Static Host Entry 3-28
Configuring an IGMP Boundary Group 3-30
Disabling and Reenabling an IGMP Boundary Group 3-31
Configuring IGMP Policies 3-32
Configuring IGMP Group Policies 3-32
Disabling and Reenabling IGMP Group Policies 3-33

Configuring IGMP Static Forwarding Policies 3-33
Disabling and Reenabling IGMP Static Forwarding Policies 3-38
Deleting IGMP 3-39

Chapter 4
Customizing DVMRP

DVMRP Concepts and Terminology 4-2
Neighbor Connections 4-2
Source Route Advertisements 4-4
How DVMRP Chooses a Route 4-5
Routing Table 4-6
Shortest-Path Trees 4-6
Tree Pruning 4-7
Customizing DVMRP Globally 4-8
Disabling and Reenabling DVMRP Globally 4-9
Setting the Update Interval 4-10
Specifying the Full Update Interval 4-10
Specifying the Triggered Update Interval 4-11
Disabling and Reenabling Tree Pruning 4-12
Setting the Route Expiration Timer 4-13
Setting the Unconfirmed Route Timer 4-15
Setting the Neighbor Report Timer 4-17
Setting the Leaf Timer 4-19
Specifying a Probe Interval 4-21
Specifying a Route Switch Interval 4-23
Estimating the Number of Routes 4-25
Specifying the Maximum Number of Routes 4-27
Logging DVMRP Messages 4-29
Customizing DVMRP on an Interface 4-30
Disabling and Reenabling DVMRP on an Interface 4-31
Enabling Multicast Migration Between DVMRP and Nonmulticast Interfaces 4-32
Receiving Nonmulticast Traffic and Forwarding As Multicast 4-32
Receiving and Forwarding Multicast Traffic 4-32
Disabling and Reenabling Multicast Support 4-33
Calculating the Cost of an Interface 4-35
Specifying a Threshold 4-37

Configuring a Forwarding Table 4-39
Specifying the Maximum Number of Table Entries 4-40
Specifying a TTL for Forwarding Table Entries 4-41
Disabling Advertisement of Local Networks 4-42
Advertising a Default Route 4-44
Listening for a Default Route 4-46
Accepting Reports from Standard DVMRP Neighbors Only 4-47
Specifying the Lifetime of a Prune Message 4-49
Configuring a DVMRP Tunnel 4-50
Supplying Addresses 4-51
Disabling and Reenabling a DVMRP Tunnel 4-53
Specifying the Encapsulation Mode for Tunneled Datagrams 4-54
Specifying the Cost 4-56
Specifying a Threshold 4-57
Configuring a Forwarding Table 4-59
Specifying the Forwarding Table Size 4-59
Specifying the Timeout for Cache Entries 4-60
Advertising a Default Route 4-62
Listening for a Default Route 4-64
Specifying an Encapsulation Mode for Control Messages 4-65
Accepting Reports from Standard DVMRP Neighbors Only 4-66
Specifying the Lifetime of a Prune Message 4-68
Configuring DVMRP Policies 4-69
Configuring DVMRP Unicast Accept Route Policies 4-69
Disabling or Reenabling DVMRP Unicast Accept Policies 4-73
Configuring DVMRP Accept Policies 4-74
Disabling or Reenabling DVMRP Accept Policies 4-78
Configuring DVMRP Announce Policies 4-79
Disabling or Reenabling DVMRP Announce Policies 4-83
Deleting DVMRP 4-84

Chapter 5
Customizing OSPF Multicast Extensions

MOSPF Concepts and Terminology 5-2
Configuring MOSPF Globally 5-4
Specifying a Forwarding Timeout Value 5-5

Specifying a Maximum Number of Queued Packets 5-6
Enabling Dynamic TTL 5-7
Enabling Multicast Migration Between MOSPF and Nonmulticast Interfaces 5-8
Forwarding Multicast Traffic from a Nonmulticast Interface to an MOSPF Interface 5-8
Forwarding Multicast Traffic from an MOSPF Interface to a Nonmulticast Interface 5-8
Configuring Multicast Forwarding on an OSPF Interface 5-9
Configuring Multicast-Capable External Routes 5-10
Configuring MOSPF Accept DVMRP Route Policies 5-11
Creating or Modifying MOSPF Accept DVMRP Route Policies 5-11
Disabling or Reenabling MOSPF Accept DVMRP Route Policies 5-12

Chapter 6
Customizing Protocol Independent Multicast

PIM Concepts and Terminology 6-2
Components of a PIM Network 6-3
Hosts 6-3
Last-Hop Router 6-3
Designated Router 6-3
Rendezvous Point (RP) Routers 6-4
Candidate RP Routers 6-4
Bootstrap Router 6-5
Candidate Bootstrap Routers 6-5
Join/Prune, Register, and Assert Messages 6-7
Join/Prune Messages 6-7
Register and Register-Stop Messages 6-7
Assert Messages 6-7
Shared Trees and Shortest-Path Trees 6-8
Shared Trees 6-8
Shortest-Path Trees 6-8
How a Receiver Joins a Multicast Group 6-10
How a Receiver Leaves a Multicast Group 6-12
How a Source Sends Multicast Packets to a Group 6-12
How the RP Switches to the Shortest-Path Tree 6-15
How the Last-Hop Router Switches to the Shortest-Path Tree 6-17

Customizing PIM Globally 6-19
Disabling and Reenabling PIM Globally 6-20
Modifying the Last-Hop Threshold 6-20
Modifying the Rendezvous Point Threshold 6-21
Specifying the Threshold Sample Interval 6-22
Setting the Default Join/Prune Interval for the Router 6-23
Modifying Neighbor Hello Messages 6-24
Modifying the Candidate BSR Configuration 6-25
Modifying the Candidate RP Configuration 6-26
Setting the Register Suppression Timer 6-27
Setting the Probe Timer 6-28
Enabling and Disabling Cisco Router Compatibility 6-29
Logging PIM Messages 6-30
Customizing PIM on an Interface 6-31
Disabling and Reenabling PIM on an Interface 6-31
Setting the Hello Interval 6-32
Setting the Cache Timeout Interval 6-33
Setting the Join/Prune Interval for an Interface 6-34
Enabling and Disabling IGMP Relay on a Downstream Router 6-35
Specifying the Local DR Priority 6-36
Deleting PIM 6-37

Chapter 7
Configuring RSVP

How RSVP Works 7-2
Configuring RSVP Globally 7-4
Disabling and Reenabling RSVP 7-4
Choosing a Slot 7-5
Logging RSVP Messages 7-6
Configuring RSVP on an Interface 7-7
Disabling and Reenabling RSVP on an Interface 7-7
Setting the RSVP Default Refresh Timer 7-8
Setting the RSVP Default Lifetime Multiplier 7-9
Setting the RSVP Refresh Blockade Multiplier 7-10
Setting the TTL Override 7-11
Setting the Route Delay Value 7-12

Enabling and Disabling UDP Encapsulation 7-13
Deleting RSVP 7-14

Chapter 8
Reserving Line Resources

About Line Resource Reservation 8-2
Resource Manager 8-2
Supported Media 8-3
How the Resource Manager Works with RSVP 8-3
Setting the Estimated Bandwidth 8-4
Setting the Reservable Bandwidth 8-5
Specifying the Traffic Queuing Algorithm 8-6
Specifying the LRM Policing Algorithm 8-7
Setting the Bandwidth Interval 8-8
Setting the Inflate Reservations Percentage 8-9
Specifying the Unreserved Policing Algorithm 8-10
Specifying the Unreserved Queue Length 8-11
Specifying the Multiline Select Algorithm 8-12
Setting the Multiline Threshold Bandwidth 8-13
Setting the Reservation Latency 8-14
Setting the Maximum Reservable Bandwidth for a Dataflow 8-15
Setting the Maximum Buffer Space for a Dataflow 8-16

Chapter 9
Configuring IGMP Relay

IGMP Relay Overview 9-2
IGMP Relay Topology 9-3
How IGMP Relay Works 9-4
Unicast Routing Protocols on the IGMP Relay Device 9-8
Routing Protocols on the Multicast Router 9-8
Enabling and Disabling IGMP Relay Globally 9-9
Specifying a Timeout Value for Multicast Table Entries 9-11
Configuring Upstream Data Forwarding 9-12
Specifying the Relay Interface Type 9-13
Configuring Unsolicited Reports on an Upstream Interface 9-16
Configuring MOSPF for Use with IGMP Relay 9-18

Configuring a DVMRP Router for Use with IGMP Relay 9-20
Configuring a Backup Multicast Router 9-22
Configuring IGMP Relay with Router Redundancy 9-23

Appendix A
Site Manager Parameters

DVMRP Parameters A-2
DVMRP Global Parameters A-2
DVMRP Interface Parameters A-7
DVMRP Tunnel Parameters A-12
IGMP Parameters A-17
IGMP Global Configuration Parameters A-17
IGMP Static Host Parameters A-21
IGMP Interface Parameters A-22
IP Configuration Parameters A-26
Resource Manager Parameters A-28
OSPF Parameters for Multicast Extensions A-35
OSPF Global Parameters A-35
OSPF Interface Parameters A-37
PIM Parameters A-37
PIM Global Configuration Parameters A-37
PIM Interface Parameters A-51
RSVP Parameters A-54
RSVP Global Parameters A-54
RSVP Interface Parameters A-56
Multicast Policy Parameters A-59
DVMRP Unicast Accept Policy Parameters A-59
DVMRP Accept Policy Parameters A-64
DVMRP Announce Policy Parameters A-69
MOSPF Accept DVMRP Route Policy Parameters A-73
IGMP Group Policy Parameters A-76
IGMP Static Forwarding Policy Parameters A-80
IGMP Boundary Group Parameters A-84

Appendix B
Troubleshooting Commands

mtrace Command B-2
mrinfo Command B-4
rsvp Command B-5

Index

Figures

Figure 1-1. Using IP Traffic Filters for Unicast to Multicast and Multicast to Unicast Data Migration 1-8
Figure 1-2. Forwarding Multicast Traffic from a Dynamic (Multicast) Network to Static Interfaces 1-9
Figure 1-3. Forwarding Multicast Traffic from a Static (Nonmulticast) Network to a Dynamic (Multicast) Network 1-10
Figure 1-4. Forwarding Multicast Traffic over Static Interfaces 1-11
Figure 3-1. Forwarding Multicast Traffic over Static Interfaces 3-34
Figure 3-2. Forwarding Multicast Traffic from a Static Network to a Dynamic Network 3-35
Figure 3-3. Forwarding Multicast Traffic from a Dynamic Network to Static Interfaces 3-36
Figure 4-1. Multicast Routers 4-3
Figure 5-1. OSPF Autonomous System 5-3
Figure 6-1. PIM Network 6-6
Figure 6-2. Shared Tree and Shortest-Path Tree 6-9
Figure 6-3. How a Receiver Joins a Multicast Group 6-11
Figure 6-4. How a Source Sends Multicast Packets to a Group 6-14
Figure 6-5. How the RP Switches to the Shortest-Path Tree 6-16
Figure 6-6. How a Last-Hop Router Switches to the Shortest-Path Tree 6-18
Figure 7-1. RSVP Path Message 7-2
Figure 7-2. RSVP Reserve Message 7-3
Figure 9-1. IGMP Relay Device 9-2
Figure 9-2. Multicast Network Topology with an IGMP Relay Device 9-4
Figure 9-3. IGMP Relay Host Queries and Responses 9-5
Figure 9-4. IGMP Relay and Upstream Multicast Data 9-6
Figure 9-5. IGMP Relay and Downstream Multicast Data 9-7
Figure 9-6. IGMP Relay Routing Protocols 9-19
Figure 9-7. DVMRP Unicast Accept Route Policy 9-21

Figure 9-8. IGMP Relay with Primary and Backup Multicast Routers 9-22
Figure 9-9. IGMP Relay with Router Redundancy 9-23

Tables

Table 1-1. Packet Migration Between Multicast and Nonmulticast Networks 1-7
Table 3-1. IGMP Message Types with Hexadecimal and Integer Values 3-10
Table 4-1. DVMRP Routing Table Entry 4-6
Table 4-2. Recommended Costs for DVMRP Interfaces 4-35
Table 4-3. Recommended TTL and Threshold Values 4-37
Table 4-4. DVMRP Unicast Accept Policy BCC Parameters 4-70
Table 4-5. DVMRP Accept Policy BCC Parameters 4-74
Table 4-6. DVMRP Announce Policy BCC Parameters 4-79
Table 9-1. IGMP Relay Forwarding Options 9-12
Table 9-2. IGMP Relay Interface Types 9-14
Table 9-3. Unsolicited IGMP Report Interval 9-16
Table B-1. mtrace Options B-2
Table B-2. mrinfo Options B-4
Table B-3. rsvp Subcommands B-5
Table B-4. Options for rsvp Subcommands B-6

Preface

This guide describes the following services and what you do to start and customize them on a Bay Networks® router:

- Internet Group Management Protocol (IGMP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Multicasting extensions to OSPF (MOSPF)
- Protocol Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)

You can use Site Manager to configure any of these services on a router. You can also use the Bay Command Console (BCC™) to configure IGMP and DVMRP. In this guide, you will find instructions for using both the BCC and Site Manager.

For instructions on how to start and use the BCC, see *Using the Bay Command Console (BCC)*; for instructions on how to start and use Site Manager, see *Configuring and Managing Routers with Site Manager.*

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network).*

Make sure that you are running the latest version of Bay Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** <*ip_address*>, you enter: **ping 192.32.10.12**
bold text	Indicates command names and options and text that you need to enter. Example: Enter **show ip** {**alerts** | **routes**}. Example: Use the **dinfo** command.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you must enter either: **show ip alerts** or **show ip routes**, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is: **show ip interfaces** [**-alerts**], you can enter either: **show ip interfaces** or **show ip interfaces -alerts**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is: **ethernet/2/1** [<*parameter*> <*value*>] **. . .** , you enter **ethernet/2/1** and as many parameter-value pairs as needed.

italic text	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.
`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

This guide uses the following acronyms:

AS	autonomous system
ASBR	AS boundary router
BDR	backup designated router
BR	border router
BSR	bootstrap router
CRM	Circuit Resource Manager
DR	designated router

DVMRP	Distance Vector Multicast Routing Protocol
FDDI	Fiber Distributed Data Interface
FIFO	first in first out
HSSI	High Speed Serial Interface
IGMP	Internet Group Management Protocol
IGMP-R	IGMP Relay
IP	Internet Protocol
IR	internal router
LRM	Line Resource Manager
LSA	link state advertisement
MBone	multicast backbone
MCT1	multichannel T1
MIB	management information base
MOSPF	multicasting extensions to OSPF
MTM	Multicast Table Manager
OSPF	Open Shortest Path First
PIM	Protocol Independent Multicast
PPP	Point-to-Point Protocol
QoS	quality of service
RFC	Request for Comments
RIP	Routing Information Protocol
RP	rendezvous point
RSVP	Resource Reservation Protocol
SPT	shortest-path tree
TTL	time to live
UDP	User Datagram Protocol

Related Publications

For more information about IP services, refer to the following publications:

- *BCC show Commands for IP Services* (Bay Networks part number 305755-A Rev 00)

  Provides descriptions of all **show** commands for IP services, including the commands that display IGMP and DVMRP configuration and statistical data.

- *Configuring IP, ARP, RIP, and OSPF Services* (Bay Networks part number 117356-E Rev 00)

  Provides a description of IP, ARP, RIP, and OSPF services and instructions for configuring them.

- *Configuring IP Exterior Gateway Protocols (BGP and EGP)* (Bay Networks part number 305752-A Rev 00)

  Provides a description of Border Gateway Protocol (BGP) and Exterior Gateway Protocol (EGP) services and instructions for configuring them.

- *Configuring GRE, NAT, RIPSO, and BFE Services* (Bay Networks part number 305753-A Rev 00)

  Provides a description of Generic Routing Encapsulation (GRE), Network Address Translation (NAT), Revised IP Security Option (RIPSO), and Blacker front-end services and instructions for configuring them.

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the Bay Networks product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase Bay Networks documentation sets, CDs, and selected technical publications through the Bay Networks Collateral Catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, contact one of the following Bay Networks Technical Solutions Centers:

Technical Solutions Center	Telephone Number
Billerica, MA	800-2LANWAN (800-252-6926)
Santa Clara, CA	800-2LANWAN (800-252-6926)
Valbonne, France	33-4-92-96-69-68
Sydney, Australia	61-2-9927-8800
Tokyo, Japan	81-3-5402-7041

Chapter 1
Multicasting and Multimedia Overview

This overview covers the following topics:

Topic	Page
Multicast Host Groups	1-2
Multicast Addresses	1-3
Internet Group Management Protocol	1-3
Distance Vector Multicast Routing Protocol	1-3
Multicasting Extensions to OSPF	1-4
Protocol Independent Multicast	1-4
Resource Reservation Protocol	1-4
Bay Networks Resource Manager	1-5
IGMP Relay	1-5
Multicast Table Manager	1-5
Multicast Migration	1-6
Using BCC show Commands to View Statistics	1-13

Multicast Host Groups

IP multicasting is a method for addressing, routing, and delivering a datagram to a collection of receivers -- called a *host group*.

Host groups can be permanent or transient:

- A *permanent host group* has a well-known, administratively assigned IP multicast group address. The address, not the membership, is permanent and defines the group. A permanent host group can consist of zero or more members.
- A *transient host group* exists only as long as it has members that need its services. IP addresses in the multicast range that are not reserved for permanent groups are available for dynamic assignment to transient host groups.

An IP multicast host group can consist of zero or more members and places no restrictions on its membership. Host members can reside anywhere; they can join and leave the group at any time; and they can be members of more than one group at the same time.

To receive a multicast message addressed to a multicast host group, a host must be a member of the group and must reside on a network where that group is registered with a local multicast router. However, any host system on any IP network can send a message to a multicast group using the group's IP multicast address: a host does not need to be a member of a group to send a multicast message to its members.

In general, hosts that are members of the same group reside on different networks. However, a range of multicast addresses (224.0.0.*x*) is reserved for groups that are locally scoped. All message traffic for these hosts remains on the local network. Hosts that belong to a group in this address range and that reside in different networks will not receive each other's message traffic.

Note: Multicast data packets are affected by traffic filters. Therefore, you must ensure that traffic filters configured on a multicast router do not prevent a host that is a member of a group from receiving packets intended for that group.

Multicast Addresses

Each host group is assigned a unique multicast address. To reach all members of the group, a sender uses the multicast address as the destination address of the datagram.

An IP Version 4 multicast address is a Class D address (the high-order bits are set to 1110) from 224.0.0.0 through 239.255.255.255.

The block of addresses from 224.0.0.1 through 224.0.0.255 is reserved for routing protocols and other low-level protocols. Multicast routers will not forward datagrams with addresses in this range.

Internet Group Management Protocol

The Internet Group Management Protocol (IGMP) has the following characteristics:

- Allows a host to register group memberships with the local queries router to receive any datagrams sent to this router and targeted to a group with a specific IP multicast address.
- Allows a router to learn the existence of group members on its directly attached networks. The router periodically sends a general group query message to each of its local networks. Any host that is a member of a multicast group identifies itself by sending a response.

For instructions on configuring IGMP, see Chapter 3, “Configuring and Customizing IGMP.”

Distance Vector Multicast Routing Protocol

The Distance Vector Multicast Routing Protocol (DVMRP) advertises shortest-path routes to multicasting *source networks* -- that is, any network containing hosts that can issue multicast datagrams. (In this respect, DVMRP is the opposite of RIP, which advertises routes to destination networks.)

For instructions on customizing DVMRP, see Chapter 4, “Customizing DVMRP.”

Multicasting Extensions to OSPF

Multicast OSPF (MOSPF) extensions enhance the OSPF protocol by providing capabilities that allow a router to forward multicast IP traffic within an OSPF Version 2 autonomous system.

For instructions on customizing MOSPF, see Chapter 5, “Customizing OSPF Multicast Extensions.”

Protocol Independent Multicast

Protocol Independent Multicast (PIM) is a multicast routing protocol that efficiently routes multicast traffic between members of multicast groups that are sparsely distributed across various regions of the Internet.

The Bay Networks implementation of PIM supports sparse mode. PIM has the following characteristics:

- Communicates with downstream members to join a shared tree by sending explicit join messages.
- Uses rendezvous points (RPs) for receivers to meet new sources. Sources announce their existence to RPs; receivers query RPs to learn about multicast sessions.
- Establishes a shortest-path tree to create a data path between sources and receivers.

For instructions on customizing PIM, see Chapter 6, “Customizing Protocol Independent Multicast.”

Resource Reservation Protocol

The Resource Reservation Protocol (RSVP) allows host systems in an IP network to reserve resources on RSVP-capable routers for unicast or multicast dataflows. (A *dataflow* is a transmission of packets from a source to one or more destinations requiring a certain QoS.)

For instructions on configuring RSVP, see Chapter 7, “Configuring RSVP.”

Bay Networks Resource Manager

The Bay Networks Resource Manager lets you define a certain percentage of a line's bandwidth as *reservable*. Applications that require a guaranteed quality of service can negotiate for the reservable bandwidth. When the router honors a reservation request, the Resource Manager allocates bandwidth from the reservable bandwidth, reducing the bandwidth available for other requests.

For more information about reserving bandwidth using the Bay Networks Resource Manager, see Chapter 8, "Reserving Line Resources."

IGMP Relay

A router configured as an IGMP Relay (IGMP-R) device provides the following services for an IP multicast router:

- Solicits multicast group membership information by sending IGMP host membership queries to hosts on its attached local networks
- Receives host membership reports and unsolicited join messages from hosts on its attached networks and forwards them to the attached multicast router
- Forwards multicast data to group members on locally attached networks

For instructions on configuring IGMP Relay, see Chapter 9, "Configuring IGMP Relay."

Multicast Table Manager

The Bay Networks Multicast Table Manager (MTM) makes it possible for different multicast protocols to work together on the same router. MTM does the following:

- Manages DVMRP and MOSPF
- Provides multicast routing support for RSVP
- Supports MOSPF special features
- Supports multicast tools for tracing routes
- Maintains a multicast forwarding cache
- Forwards multicast traffic

Multicast Migration

You can enable the flow of multicast traffic over either multicast (DVMRP or MOSPF) or nonmulticast, IGMP static router interfaces. To enable the transfer of packets between multicast and nonmulticast networks, you must create one or more of the following:

- IP traffic filters
- IGMP static forwarding policies
- Multicast protocol policies (DVMRP or MOSPF)

You must configure IGMP on any interface running a multicast protocol, as well as on any static interface over which you want to transfer multicast traffic.

You can also allow unicast packets to travel as multicast and multicast packets as unicast between multicast and nonmulticast networks. Table 1-1 provides an overview of how different packet types can travel between multicast and nonmulticast networks.

Table 1-1. Packet Migration Between Multicast and Nonmulticast Networks

Router Receives This Type of Packet	On This Type of Interface	Forwarding Action and How to Enable
Unicast or broadcast	Multicast	The multicast protocol running on the interface forwards the packet to a multicast destination address or a list of multicast destination addresses based on a configured IP traffic filter. (The IP traffic filter converts the unicast or broadcast packets to multicast.) See 1-1Figure 1-1.
Multicast	Multicast	The multicast protocol running on the router forwards the packet on to either: • A multicast configured outbound interface, based on the multicast protocol decisions. • A nonmulticast, IGMP static configured outbound circuit. In Site Manager, you must set the IGMP static forwarding entries policy for *Dynamic to Static* forwarding mode. See Figure 1-2.
Multicast	Nonmulticast, IGMP static configured	If you set the IGMP static forwarding policy for *Static to Dynamic* forwarding mode, and if multicast protocols are running on the outbound interfaces, the router forwards multicast packet traffic to a multicast enabled network. You must also set the IGMP interface parameter Static Forward Cache Lifetime to a value in accordance with the particular multicast protocol (DVMRP or MOSPF) that is running on the outbound interface. See Figure 1-3. If you set the IGMP static forwarding policy for *Static* forwarding mode, the router forwards the multicast traffic to a nonmulticast, static configured interface. See Figure 1-4.

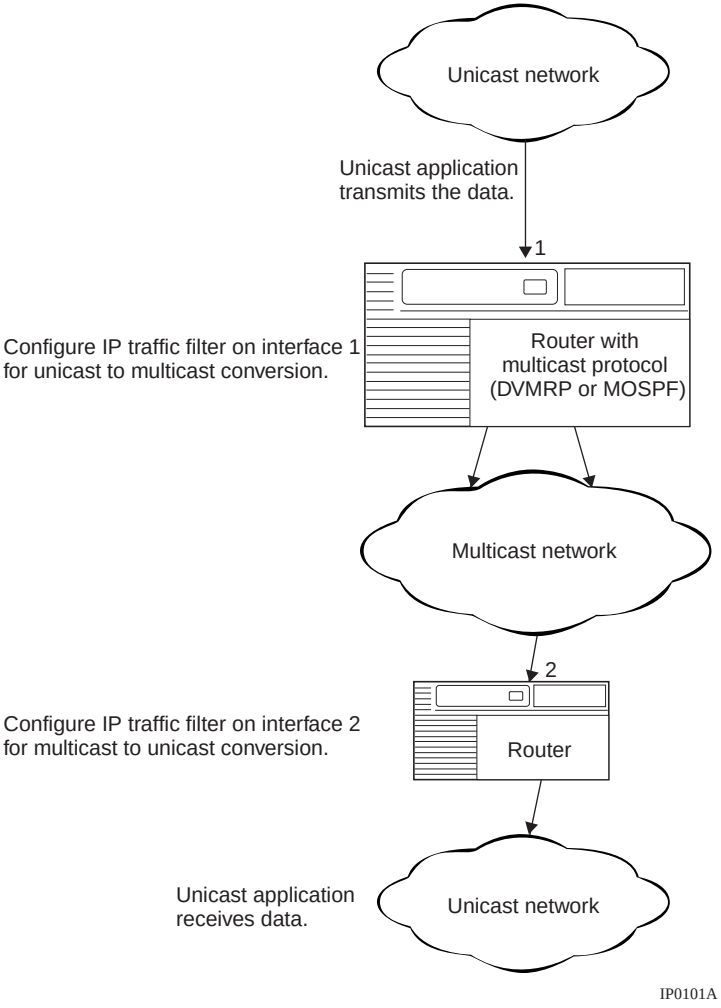

Figure 1-1. Using IP Traffic Filters for Unicast to Multicast and Multicast to Unicast Data Migration

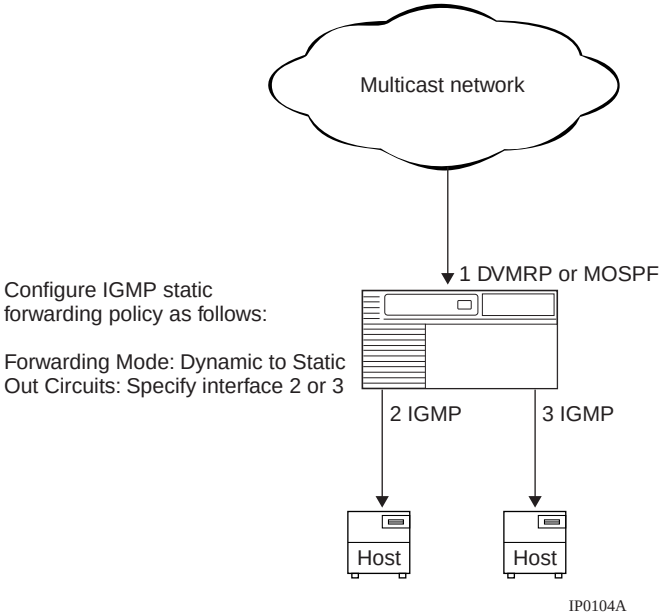

Figure 1-2. Forwarding Multicast Traffic from a Dynamic (Multicast) Network to Static Interfaces

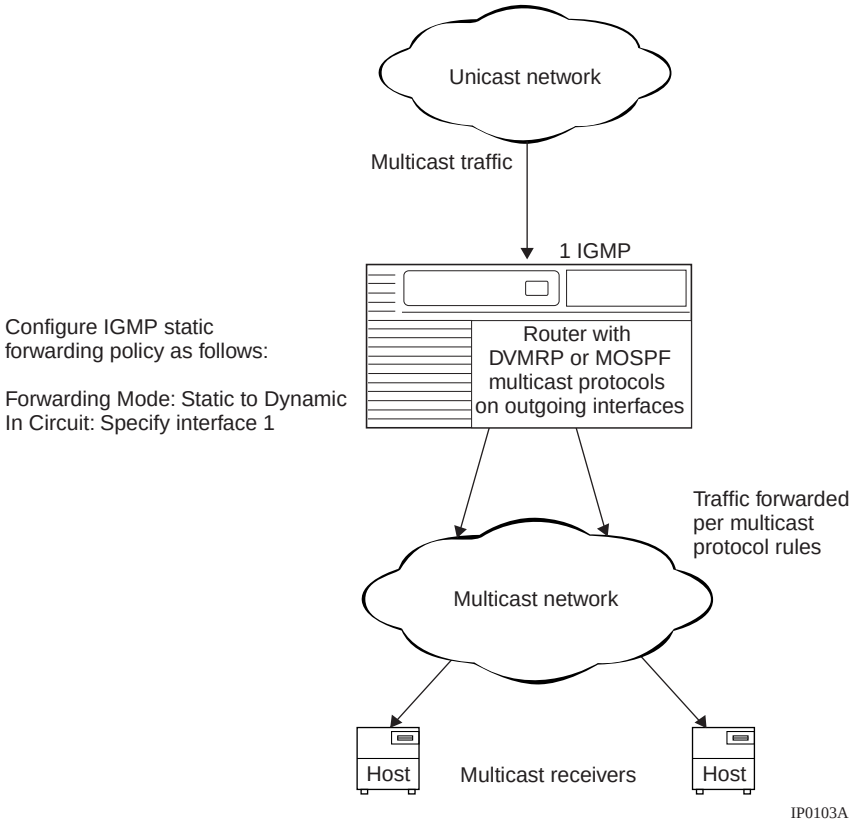

Figure 1-3. Forwarding Multicast Traffic from a Static (Nonmulticast) Network to a Dynamic (Multicast) Network

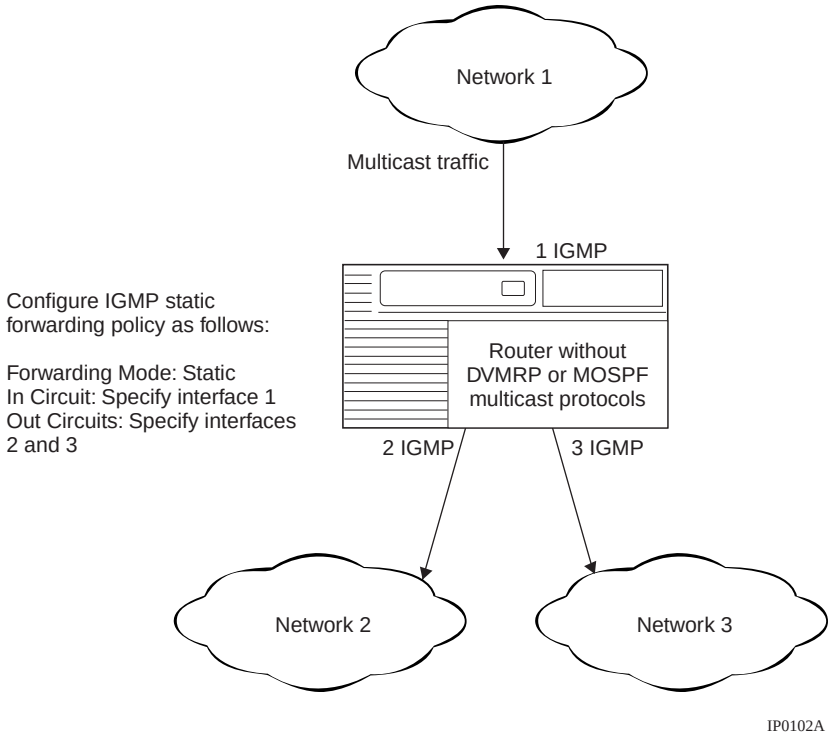

Figure 1-4. Forwarding Multicast Traffic over Static Interfaces

Configuring Multicast Migration

To configure your network to transfer both multicast and nonmulticast traffic using multicast migration tools, follow these steps:

1. **Make sure that IGMP is configured on the router interfaces that will be receiving or forwarding the multicast or nonmulticast traffic.**

   IGMP is automatically enabled on any interface that you configure with DVMRP or MOSPF using Site Manager. For instructions on starting IGMP on a router interface, see “Starting IGMP” on page 2-2.

2. **Configure an IP traffic filter if you need to convert packets from unicast to broadcast, or from broadcast to unicast. You must also configure an IP traffic filter to convert packet data from multicast to unicast/broadcast, or from unicast/broadcast to multicast.**

   To convert packets from unicast/broadcast to multicast, a multicast protocol must be running on the incoming interface. For instructions on how to configure IP traffic filters, see *Configuring Traffic Filters and Protocol Prioritization*.

3. **Configure an IGMP static forwarding policy using Site Manager for the interfaces that are static (nonmulticast) or dynamic (multicast).**

   For instructions, see “Configuring IGMP Static Forwarding Policies” on page 3-33.

4. **Depending on whether the multicast protocol on your router interface is DVMRP or MOSPF:**

   - See “Enabling Multicast Migration Between DVMRP and Nonmulticast Interfaces” on page 4-32.
   - See “Enabling Multicast Migration Between MOSPF and Nonmulticast Interfaces” on page 5-8.

5. **You may need to set policy filters to identify acceptable gateways, interfaces, tunnels, and networks for passing traffic using IGMP, DVMRP, and MOSPF. For example, you may need to specify an incoming network address to which a user-defined multicast routing policy applies.**

For instruction on how to configure policies for these multicast protocols:

- See “Configuring IGMP Policies” on page 3-32.
- See “Configuring DVMRP Policies” on page 4-69.
- See “Configuring MOSPF Accept DVMRP Route Policies” on page 5-11.

Using BCC show Commands to View Statistics

As you configure your router interfaces with multicast protocols, you can view configuration and statistical data about your networks using the following BCC **show** commands:

- **show dvmrp**
- **show igmp**

For example, the following command displays summary information about the DVMRP configuration:

```
bcc> show dvmrp summary
State = Up
Pruning = Enabled
Full Update Interval = 60
Trigger Update Interval = 5
Leaf Timeout = 200
Neighbor Timeout = 140
Neighbor Probe Interval = 10
Switch Timeout = 140
Route Expiration Timeout = 200
Unconfirmed Route Timeout = 340
estimated Routes = 25
Actual Routes = 8
```

To display online Help for available **show** options, use the question mark (?) command. For example:

```
box# show dvmrp ?
   caches       neighbors    summary
   interfaces   routes       tunnels
```

For more information, see *BCC show Commands for IP Services*.

Chapter 2
Starting Multicasting and Multimedia Services

This chapter explains how to perform a basic configuration -- that is, a configuration using all available defaults -- for the IP multicast services described in this guide.

Topic	Page
Starting IGMP	2-2
Starting DVMRP	2-4
Starting MOSPF	2-6
Starting PIM	2-7
Starting RSVP	2-10

Starting IGMP

IGMP is required for all types of multicasting. If you want the router to receive and forward multicast packets (that is, packets with destination addresses from 224.0.0.255 through 239.255.255.255), IGMP must be running on the slot and circuit -- even if the circuit is a point-to-point circuit that will not be involved in IGMP group queries and join messages.

You can start IGMP using the BCC or Site Manager.

Note: If you plan to start DVMRP, MOSPF, or PIM using Site Manager, go to the appropriate section in this chapter. Site Manager automatically enables IGMP when you configure DVMRP, MOSPF, or PIM.

Using the BCC

To start IGMP on an interface with default values, navigate to the IP interface prompt (for example, **box; ethernet/2/2; ip/1.2.3.4/255.255.255.0**) and enter **igmp**:

```
ip/1.2.3.4/255.255.255.0# igmp
igmp/1.2.3.4#
```

Using Site Manager

When you configure any multicast protocol described in this guide (DVMRP, MOSPF, or PIM), Site Manager automatically configures IGMP on the slot and circuit.

To start IGMP on a router interface that does not have another multicast protocol configured:

1. **Configure a circuit on a slot and connector.**
2. **Configure an IP interface on the circuit.**
3. **Add IGMP to the interface.**

For information and instructions on using Site Manager to configure a circuit on a slot and connector, see *Configuring WAN Line Services* or *Configuring Ethernet, FDDI, and Token Ring Services.*

When you have successfully configured the circuit, the Select Protocols window opens. Proceed as follows:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, choose the following protocols: • **IP** • **IGMP/IGMP Relay**	
2. Click on **OK**.	The IP Configuration window opens.
3. Set the following parameters: • **IP Address** • **Subnet Mask** • **Transmit Bcast Addr** • **UnNumbered Assoc Address** Click on **Help** or see the parameter descriptions beginning on page A-26.	
4. Click on **OK**.	If this is the first IGMP interface on the router, the Initial IGMP Global Configuration window opens. Otherwise, you return to the Configuration Manager window.
5. In the Initial IGMP Global Configuration window, click on **Save** to accept the default values.	You return to the Configuration Manager window.

IGMP is now running on the router with default values for all interface parameters. You can customize IGMP by modifying IGMP parameters. For information and instructions, see Chapter 3, “Configuring and Customizing IGMP.”

Starting DVMRP

You can start DVMRP using either the BCC or Site Manager. When you configure DVMRP on an IP interface, DVMRP is also configured globally on the router.

If you follow the instructions provided below, DVMRP will be running on the router with default values for all global and interface parameters. You customize DVMRP by modifying DVMRP parameters. For information and instructions, see Chapter 4, "Customizing DVMRP."

Using the BCC

To start DVMRP on an interface with default values, you must first configure IGMP. Navigate to the IP or IGMP interface prompt (for example, **box; ethernet/2/2; ip/1.2.3.4/255.255.255.0; igmp**) and enter:

dvmrp

For example, the following command sequence configures IGMP and DVMRP on IP interface 1.2.3.4/255.255.255.0:

```
ip/1.2.3.4/255.255.255.0# igmp
igmp/1.2.3.4# dvmrp
dvmrp/1.2.3.4#
```

If you try to configure DVMRP without first configuring IGMP, you will see the following message:

```
Configuration of Igmp is required.
```

Using Site Manager

To start DVMRP on the router:

1. **Configure a circuit on a slot and connector.**
2. **Configure an IP interface on the circuit.**
3. **Add DVMRP to the IP interface.**

For information and instructions on using Site Manager to configure a circuit on a slot and connector, see *Configuring WAN Line Services* or *Configuring Ethernet, FDDI, and Token Ring Services*.

When you have successfully configured the circuit, the Select Protocols window opens. Proceed as follows:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, choose the following protocols: • **IP** • **DVMRP**	When you select DVMRP, IGMP is automatically selected.
2. Click on **OK**.	The IP Configuration window opens.
3. Set the following parameters: • **IP Address** • **Subnet Mask** • **Transmit Bcast Addr** • **UnNumbered Assoc Address** Click on **Help** or see the parameter descriptions beginning on page A-26.	
4. Click on **OK**.	If this is the first DVMRP interface on the router, the DVMRP Global Parameters window opens. Otherwise, you return to the Configuration Manager window.
5. In the DVMRP Global Parameters window, click on **Save** to accept the default values.	If this is the first IGMP interface on the router, the Initial IGMP Global Configuration window opens. Otherwise, you return to the Configuration Manager window.
6. In the Initial IGMP Global Configuration window, click on **Save** to accept the default values.	You return to the Configuration Manager window.

DVMRP is now running on the router with default values for all global and interface parameters. IGMP is also automatically enabled.

Starting MOSPF

MOSPF is a multicasting extension of OSPF. To start MOSPF, you must add OSPF to an IP interface and enable MOSPF multicast extensions to support one of the following types of multicasting:

- Intra-area multicasting
- Intra-area and inter-area multicasting
- Intra-area and inter-AS multicasting
- All multicasting

For more information about MOSPF multicasting types and instructions on customizing MOSPF, see Chapter 5, “Customizing OSPF Multicast Extensions.”

To enable MOSPF on a router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. Configure OSPF on the router as described in *Configuring IP, ARP, RIP, and OSPF Services*.	
2. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
3. Choose **IP**.	The IP menu opens.
4. Choose **OSPF/MOSPF**.	The OSPF menu opens.
5. Choose **Global**.	The Edit OSPF Global Parameters window opens.
6. Click on the **Multicast Extensions** parameter. Click on **Help** or see the parameter description on page A-35.	
7. Click on **Values** to select the type of MOSPF that you want to configure, and then click on **OK**.	If this is the first IGMP interface on the router, the Initial IGMP Global Configuration window opens. Otherwise, you return to the Configuration Manager window.
8. In the Initial IGMP Global Configuration window, click on **Save** to accept the default values.	You return to the Configuration Manager window.

MOSPF is now running on the router with default values for all parameters. IGMP is also automatically enabled.

Starting PIM

This section describes how to create a basic PIM configuration by specifying values for required parameters only and accepting defaults values for all other parameters.

For an introduction to PIM, see "PIM Concepts and Terminology" on page 6-2.

Configuration Prerequisites

Before you can configure PIM on a router, you must configure the router as follows:

- Disable IGMP Relay on the router on which you want to configure PIM.

  PIM and IGMP Relay cannot be configured on the same router. For instructions on how to disable IGMP Relay, see "Enabling and Disabling IGMP Relay Globally" on page 9-9.

- Delete DVMRP and MOSPF from the interface on which you want to configure PIM.

  PIM, DVMRP, and MOSPF cannot be configured on the same interface.

- Configure a unicast protocol (RIP or OSPF) on the same interface on which you want to configure PIM.

  PIM requires a unicast protocol to propagate multicast traffic within the network. For information about configuring unicast protocols, see *Configuring IP, ARP, RIP, and OSPF Services.*

Starting PIM on the Router

To start PIM on the router:

1. **Configure a circuit on a slot and connector.**
2. **Configure an IP interface on the circuit.**
3. **Add PIM to the IP interface.**
4. **Configure a router to act as a bootstrap router.**
5. **Configure a router to act as a rendezvous point router.**

For information and instructions on configuring a circuit on a slot and connector, see *Configuring WAN Line Services* or *Configuring Ethernet, FDDI, and Token Ring Services*.

When you have successfully configured the circuit, the Select Protocols window opens. Proceed as follows:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, choose the following protocols: • **IP** • **PIM**	When you select PIM, IGMP is automatically configured on the slot and circuit.
2. Click on **OK**.	The IP Configuration window opens.
3. Set the following parameters: • **IP Address** • **Subnet Mask** • **Transmit Bcast Addr** • **UnNumbered Assoc Address** Click on **Help** or see the parameter descriptions beginning on page A-26.	
4. Click on **OK**.	The PIM Global Configuration window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Set the following parameters to configure a bootstrap router and a rendezvous point router: • **Candidate BSR** • **Candidate BSR IP Address** • **Candidate RP** • **Candidate RP IP Address** • **Candidate RP Group/Mask** Click on **Help** or see the parameter descriptions beginning on page A-41.	
6. Click on **OK**.	The Initial IGMP Global Configuration window opens.
7. Accept the default values by clicking on **Save**.	You return to the Configuration Manager window.

PIM is now running on the router with default values for all global and interface parameters. You can customize PIM by modifying PIM parameters. For information and instructions, see Chapter 6, “Customizing Protocol Independent Multicast.”

Starting RSVP

To start RSVP on the router using Site Manager:

1. **Configure a circuit on a slot and connector.**
2. **Configure an IP interface on the circuit.**
3. **Add RSVP to the IP interface.**

For information and instructions on using Site Manager to configure a circuit on a slot and connector, see *Configuring WAN Line Services* or *Configuring Ethernet, FDDI, and Token Ring Services*.

When you have successfully configured the circuit, the Select Protocols window opens. Proceed as follows:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, choose the following protocols: • **IP** • **RSVP**	
2. Click on **OK**.	The IP Configuration window opens.
3. Set the following parameters: • **IP Address** • **Subnet Mask** • **Transmit Bcast Addr** • **UnNumbered Assoc Address** Click on **Help** or see the parameter descriptions beginning on page A-26.	
4. Click on **OK**.	The Initial RSVP Global Configuration window opens.
5. Click on **Save**.	Site Manager asks you whether you want to create line resources.
6. Click on **Yes**.	The Edit Line Resources window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
7. Set the following parameters: • **Estimated Bandwidth** • **Reservable Bandwidth** Click on **Help** or see the parameter descriptions beginning on page A-28.	
8. Click on **OK**.	You return to the Configuration Manager window.

RSVP is now running on the router with default values for all parameters. You customize RSVP by modifying RSVP parameters. For information and instructions, see Chapter 7, “Configuring RSVP.”

Chapter 3
Configuring and Customizing IGMP

This chapter covers the following topics describing the Internet Group Management Protocol (IGMP):

Topic	Page
IGMP Concepts and Terminology	3-2
Customizing IGMP Globally	3-4
Customizing IGMP on an Interface	3-15
Configuring a Static Host Entry	3-28
Configuring an IGMP Boundary Group	3-30
Disabling and Reenabling an IGMP Boundary Group	3-31
Configuring IGMP Policies	3-32
Deleting IGMP	3-39

IGMP Concepts and Terminology

The Internet Group Management Protocol (IGMP) allows hosts to communicate their group memberships to their local queries router and to receive any datagrams sent to this router and targeted to a group with a specific IP multicast address. Bay Networks routers support IGMP Version 2.

A router communicates with the hosts on a local network by sending IGMP queries. Hosts respond by issuing IGMP reports.

This section covers the following topics:

Topic	Page
IGMP Queries	3-2
IGMP Host Reports	3-3
Host Leave Messages	3-3

IGMP Queries

A router running IGMP periodically sends host membership queries to its attached local networks. Routers that conform to RFC 1112 generate Version 1 queries. Bay Networks routers configured with IGMP generate Version 2 queries.

If multiple IGMP routers exist on the network, Bay Networks routers designate one router to send host member queries, using the following rules:

- Choose a router that generates Version 1 queries over a router that generates Version 2 queries.
- Choose the router with the lowest IP address.

IGMP Host Reports

A host that receives a membership query from a local router can respond with a *host membership report* for each joined multicast group. A host that receives a query delays its reply by a random interval and listens for a reply from any other host in the same host group.

For example, consider a network that includes two host members of the same multicast group -- host A and host B. The router sends out a host membership query on the local network. Both host A and host B receive the query and listen on the network for a host membership report. Host B's delay time expires first, so it responds to the query with a membership report. Hearing the response, host A does not send a report of its own for the same group.

Each query from a router to a host includes a code field. IGMP inserts a value -- *n* -- into this field specifying the maximum time in tenths of a second within which the host must issue a reply. The host uses this value to calculate a random value between 0 and *n* tenths of a second for the period that it waits before sending a response.

If at least one host on the local network specifies that it is a member of a given group, the router will forward to that network all datagrams bearing the group's multicast address.

Upon initialization, the host may immediately issue a report for each of its supported multicast groups. The router accepts and processes these asynchronous reports the same way it accepts requested reports.

Once in a steady state, hosts and routers communicate in a way that minimizes the exchange of queries and reports.

Host Leave Messages

When a Version 2 host leaves a group, it issues a *host leave message.* The multicast router on the network issues a group-specific query to determine whether there are other group members on the network. If no host responds to the query, the router assumes that no members belonging to that group exist on that interface.

Customizing IGMP Globally

When you configure IGMP on the router, IGMP is automatically enabled with default values for all global parameters. You customize global IGMP by modifying parameters as described under the following topics:

Topic	Page
Enabling and Disabling IGMP Globally	3-5
Estimating the Number of Groups	3-6
Specifying a Version Threshold Time	3-8
Logging IGMP Messages	3-10
Enabling Join Acknowledgments	3-12
Specifying a Forwarding Cache Limit	3-13
Accepting a Nonlocal Report	3-14

Enabling and Disabling IGMP Globally

When you configure IGMP on the router, IGMP is automatically enabled. You can use the BCC or Site Manager to disable and reenable IGMP on the router.

Using the BCC

To disable or reenable IGMP on the router, navigate to the global IGMP prompt (for example, **box; ip; igmp**) and enter:

state <*state*>

state is one of the following:

enabled (default)
disabled

Using Site Manager

To enable or disable IGMP on the router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Global**.	The IGMP Global Configuration window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-17.	
6. Click on **Save**.	You return to the Configuration Manager window.

Estimating the Number of Groups

By default, IGMP estimates that 20 multicast groups will be simultaneously active on this router. This estimate allows the router to use memory efficiently; exceeding this size during router operation will not cause an error but may cause the router to consume more memory than required.

Note: You do not need to include in the count any group from 224.0.0.0 through 224.0.0.255.

You can use the BCC or Site Manager to supply an estimate from 5 through 65,535 groups.

Using the BCC

To specify the estimated number of multicast groups, navigate to the global IGMP prompt (for example, **box; ip; igmp**) and enter:

estimated-groups *<groups>*

groups is an integer from 5 through 65,535.

Using Site Manager

To estimate the number of groups, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Global**.	The IGMP Global Configuration window opens.
5. Set the **Estimated Groups** parameter. Click on **Help** or see the parameter description on page A-17.	
6. Click on **Save**.	You return to the Configuration Manager window.

Specifying a Version Threshold Time

By default, 540 seconds (9 minutes) can elapse after IGMP detects a Version 1 query before IGMP tries to become the designated querier.

You can use the BCC or Site Manager to specify a version threshold time from 1 through 65,535 seconds (18 hours, 12 minutes, and 15 seconds). The value that you specify should be greater than the Version 1 query rate of all IGMP speakers on all networks directly connected to the router.

Using the BCC

To specify a version threshold time, navigate to the global IGMP prompt (for example, **stack; ip; igmp**) and enter:

version-threshold *<threshold>*

threshold is the number of seconds from 1 through 65,535.

For example, the following command sets the version threshold time to 500 seconds (8 minutes, 20 seconds):

```
igmp# version-threshold 500
igmp#
```

Using Site Manager

To specify a version threshold time, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Global**.	The IGMP Global Configuration window opens.
5. Set the **Version Threshold Time** parameter. Click on **Help** or see the parameter description on page A-18.	
6. Click on **Save**.	You return to the Configuration Manager window.

Logging IGMP Messages

By default, IGMP does not log messages. You can use the BCC or Site Manager to specify the message types that you want IGMP to log.

Using the BCC

To specify the types of messages that IGMP logs, navigate to the global IGMP prompt (for example, **box; ip; igmp**) and enter:

debug-log-flag *<flag>*

flag is an integer or hexadecimal value equivalent to a message type (Table 3-1).

Table 3-1. IGMP Message Types with Hexadecimal and Integer Values

Message Type	Integer Value	Hexadecimal Value
No messages	0	0x0
Received IGMP protocol (join/leave) packets	1	0x00000001
Sent IGMP messages	2	0x00000002
Received multicast protocol packets	4	0x00000004
Mtrace utility related log messages	8	0x00000008
Configuration related log messages	16	0x00000010
Interaction with multicast protocols	32	0x00000020
Interaction with RSVP	64	0x00000040
MTM forwarding cache related log messages	128	0x00000080
IGMP Relay related log messages	256	0x00000100

Using Site Manager

To configure message logging, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Global**.	The IGMP Global Configuration window opens.
5. Set the **Debug** parameter. Click on **Help** or see the parameter description on page A-19.	
6. Click on **Save**.	You return to the Configuration Manager window.

Enabling Join Acknowledgments

By default, IGMP does not respond with an acknowledgment to join requests from host groups.

Using Site Manager, you can configure IGMP globally to respond to a join request by sending an IGMP query to the group.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Global**.	The IGMP Global Configuration window opens.
5. Set the **Join Ack Enable** parameter. Click on **Help** or see the parameter description on page A-18.	
6. Click on **Save**.	You return to the Configuration Manager window.

Note: This is a proprietary Bay Networks function. It is not part of standard IGMP.

Specifying a Forwarding Cache Limit

By default, IGMP allows a maximum of 512 entries in the Multicast Table Manager (MTM) forwarding cache. This number affects all multicasting protocols.

The MTM cache must be at least as large as individual routing protocol caches (for example, the DVMRP cache).

You can use Site Manager to set the forwarding cache to a different value.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Global**.	The IGMP Global Configuration window opens.
5. Set the **Forward Cache Limit** parameter. Click on **Help** or see the parameter description on page A-18.	
6. Click on **Save**.	You return to the Configuration Manager window.

Accepting a Nonlocal Report

By default, IGMP rejects join and leave messages from nonlocal networks. You can use the BCC or Site Manager to control the way IGMP handles nonlocal reports.

Using the BCC

To specify the way IGMP handles nonlocal reports, navigate to the global IGMP prompt (for example, **stack; ip; igmp**) and enter:

ignore-nonlocal-report *<action>*

action is one of the following:

ignore (default)
accept

For example, the following command causes IGMP to accept join and leave messages from nonlocal networks:

```
igmp# ignore-nonlocal-report accept
igmp#
```

Using Site Manager

To specify the way IGMP handles nonlocal reports, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Global**.	The IGMP Global Configuration window opens.
5. Set the **Nonlocal Reports** parameter. Click on **Help** or see the parameter description on page A-20.	
6. Click on **Save**.	You return to the Configuration Manager window.

Customizing IGMP on an Interface

When you add IGMP to an IP interface, IGMP is enabled with default values for all interface parameters. You customize IGMP on the interface by modifying parameters as described under the following topics:

Topic	Page
Enabling and Disabling IGMP on an Interface	3-16
Specifying Query Suppression	3-17
Specifying a Query Rate	3-19
Specifying a Membership Timeout Interval	3-21
Specifying a Designated Router Timeout Interval	3-22
Specifying a Maximum Host Response Time	3-24
Specifying the Lifetime of an Mtrace Cache Entry	3-26
Specifying the Static Forward Cache Lifetime	3-27

Enabling and Disabling IGMP on an Interface

When you add IGMP to an IP interface, IGMP is automatically enabled on the interface.

Note: IGMP is required for multicasting to function on the interface.

You can use the BCC or Site Manager to disable and reenable IGMP on the interface.

Using the BCC

To disable or reenable IGMP on an IP interface, navigate to the IGMP prompt for the interface (for example, **box; ethernet/2/1; ip/2.2.2.2/255.255.255.0; igmp**) and enter:

state *<state>*

state is one of the following:

enabled (default)
disabled

Using Site Manager

To enable and disable IGMP on an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Interfaces**.	The IGMP Interface Parameters window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-22.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying Query Suppression

In the Bay Networks multicast implementation, configuring IGMP on an interface does the following:

- The interface is used for forwarding multicast traffic.
- IGMP is running on the interface.

If you configured IGMP on an interface only for the purpose of forwarding multicast traffic, you should disable the sending of IGMP group membership queries.

You can use the BCC or Site Manager to suppress queries. By default, IGMP sends queries.

Using the BCC

To disable or reenable the sending of IGMP queries, navigate to the IGMP prompt for the interface (for example, **box; ethernet/2/1; ip/2.2.2.2/255.255.255.0; igmp**) and enter:

suppress-query {**yes** | **no**}

For example, the following command suppresses the sending of IGMP queries on IP interface 2.2.2.2:

```
igmp/2.2.2.2/3# suppress query yes
igmp/2.2.2.2/3#
```

Using Site Manager

To specify query suppression on an IGMP interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Interfaces**.	The IGMP Interface Parameters window opens.
5. Set the **Query Suppression** parameter. Click on **Help** or see the parameter description on page A-25.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying a Query Rate

By default, IGMP sends a group membership query on the interface every 120 seconds (2 minutes). You can use the BCC or Site Manager to disable queries or to specify a query rate from 1 through 4096 seconds (1 hour, 8 minutes, and 16 seconds).

Specifying 0 disables queries only. The router still forwards multicast datagrams on this circuit.

Note: If another IGMP router on this network has assumed the query role, this router will not send out queries unless it has not heard of any queries within the number of seconds specified by the designated router timeout parameter (see "Specifying a Designated Router Timeout Interval" on page 3-22).

Using the BCC

To specify a query rate or to disable queries, navigate to the IGMP prompt for the interface (for example, **box; ethernet/2/1; ip/2.2.2.2/255.255.255.0; igmp**) and enter:

query-rate *<rate>*

rate is the number of seconds from 0 (disabling queries) through 4096.

For example, the following command specifies a query rate of 300 seconds (5 minutes):

```
igmp/2.2.2.2/3# query-rate 300
igmp/2.2.2.2/3#
```

Using Site Manager

To specify a query rate, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Interfaces**.	The IGMP Interface Parameters window opens.
5. Set the **Interface Query Rate** parameter. Click on **Help** or see the parameter description on page A-23.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying a Membership Timeout Interval

By default, a local group membership is valid for 260 seconds (4 minutes, 20 seconds) without the receipt of a subsequent report for that group.

You can use the BCC or Site Manager to specify a timeout interval from 50 to 8192 seconds (2 hours, 16 minutes, and 32 seconds).

Using the BCC

To set the membership timeout interval, navigate to the IGMP prompt for the IP interface (for example, **box; ethernet/2/1; ip/2.2.2.2/255.255.255.0; igmp**) and enter:

membership-timeout *<seconds>*

seconds is the number of seconds from 50 through 8192.

For example, the following command specifies a membership timeout interval of 300 seconds (5 minutes):

```
igmp/2.2.2.2/3# membership-timeout 300
igmp/2.2.2.2/3#
```

Using Site Manager

To specify a membership timeout interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Interfaces**.	The IGMP Interface Parameters window opens.
5. Set the **Interface Membership Timeout** parameter. Click on **Help** or see the parameter description on page A-23.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying a Designated Router Timeout Interval

By default, 140 seconds (2 minutes, 20 seconds) can elapse after the last host query message before IGMP considers the designated router to be down.

You can use the BCC or Site Manager to specify a router timeout interval from 10 through 8192 seconds (2 hours, 16 minutes, and 32 seconds). The value you specify should be greater than the query rate of all IGMP routers on the network. The suggested value is two times the value of the interface query rate plus 20 seconds.

Using the BCC

To specify a designated router timeout interval, navigate to the IGMP prompt for the interface (for example, **box; ethernet/2/1; ip/2.2.2.2/255.255.255.0; igmp**) and enter:

dr-timeout *<seconds>*

seconds is an interval from 10 through 8192 seconds.

For example, the following command sets the router timeout interval to 200 seconds (3 minutes, 20 seconds):

```
igmp/2.2.2.2/3# dr-timeout 200
igmp/2.2.2.2/3#
```

Using Site Manager

To specify a designated router timeout interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Interfaces**.	The IGMP Interface Parameters window opens.
5. Set the **Designated Router Timeout** parameter. Click on **Help** or see the parameter description on page A-24.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying a Maximum Host Response Time

By default, a host must wait 100 tenths of a second before responding to a query. IGMP places this value in the code field of an IGMP query.

You can use the BCC or Site Manager to specify a value from 1 to 100 tenths of a second.

Using the BCC

To specify the maximum host response time, navigate to the IGMP prompt for the interface (for example, **box; ethernet/2/1; ip/2.2.2.2/255.255.255.0; igmp**) and enter:

max-host-response *<time>*

time is an integer from 1 through 100 specifying the response time in tenths of a second.

For example, the following command sets the maximum host response time to 25 tenths of a second:

```
igmp/2.2.2.2/3# max-host-response 25
igmp/2.2.2.2/3#
```

Using Site Manager

To specify the maximum host response time, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Interfaces**.	The IGMP Interface Parameters window opens.
5. Set the **Max Host Response Time** parameter. Click on **Help** or see the parameter description on page A-24.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying the Lifetime of an Mtrace Cache Entry

IGMP creates entries in the forwarding cache specifically for the Mtrace utility. By default, IGMP keeps these entries in the forwarding cache for a maximum of 30 seconds.

You can use the BCC or Site Manager to specify a different lifetime value from 30 through 8192 seconds (2 hours, 16 minutes, and 32 seconds).

Using the BCC

To specify the lifetime value for the Mtrace cache entries, navigate to the IGMP prompt for the interface (for example, **box; ethernet/2/1; ip/2.2.2.2/255.255.0.0; igmp**) and enter:

mtrace-lifetime *<seconds>*

seconds is an interval from 30 through 8192 seconds.

For example, the following command sets the Mtrace cache entry lifetime to 60 seconds:

```
igmp/2.2.2.2/3# mtrace-lifetime 60
igmp/2.2.2.2/3#
```

Using Site Manager

To specify the lifetime of an Mtrace cache entry, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Interfaces**.	The IGMP Interface Parameters window opens.
5. Set the **Mtrace Entry Lifetime** parameter. Click on **Help** or see the parameter description on page A-24.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying the Static Forward Cache Lifetime

The static forwarding cache lifetime is the number of seconds that the Multicast Table Manager (MTM) keeps entries in its cache. The default value is 216 seconds (3 minutes, 36 seconds).

When you configure an IGMP static forwarding policy to accept multicast traffic on a nonmulticast interface and then forward it out a multicast interface (static to dynamic forwarding mode), you must modify the static forward cache lifetime on the inbound static interface based on the outbound multicast protocol configured on the outbound interface.

You can set this value from 80 through 7200 seconds, based on the multicast protocol configured on the outbound router interface. A typical value for DVMRP is 7200, and for MOSPF, 600.

For instructions on configuring IGMP static forwarding policies, see “Configuring IGMP Static Forwarding Policies” on page 3-33.

To set the static forward cache lifetime, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Interfaces**.	The IGMP Interface Parameters window opens.
5. Set the **Static Forward Cache Lifetime** parameter. Click on **Help** or see the parameter description on page A-25.	The IGMP Interface Parameters window opens.
6. Click on **Apply,** then click on **Done**.	You return to the Configuration Manager window.

Configuring a Static Host Entry

A network may include a member of a multicast group that is unable to register its group membership with the local IGMP router, for example, a host that is a member of a multicast group but that is not running IGMP.

In this situation, you can register the group member's network statically on the router.

A registration entry includes:

- A group address
- An address prefix length
- A circuit name

To configure a static host entry, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Static Groups**.	The IP IGMP Static Groups window opens.
5. Click on **Add**.	The IGMP Static Group window opens.
6. Set the following parameters: • **Group Address** • **Prefix Length** • **Circuit Name** Click on **Help** or see the parameter descriptions beginning on page A-22.	
7. Click on **OK**.	You return to the IP IGMP Static Groups window.
8. Click on **Done**.	You return to the Configuration Manager window.

Configuring an IGMP Boundary Group

You configure an IGMP boundary group by supplying a range of multicast group addresses (expressed as an address and a prefix) and a list of IP interfaces. No multicast group address that falls within the range that you specify is accepted or forwarded on the interfaces that you specify.

For more information about groups, see “Multicast Host Groups” on page 1-2.

You can use Site Manager to define an IGMP boundary group.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Admin Scope**.	The IP IGMP Admin Scope window opens.
5. Click on **Add**.	The IGMP Admin Scope window opens.
6. Set the following parameters: • **Group Address** • **Prefix Length** • **Circuit List** • **Tunnel List** Click on **Help** or see the parameter descriptions beginning on page A-84.	
7. Click on **OK**.	You return to the IP IGMP Admin Scope window.
8. Click on **Done**.	You return to the Configuration Manager window.

Disabling and Reenabling an IGMP Boundary Group

When you configure an IGMP boundary group, by default the boundary group is enabled.

To disable or reenable an IGMP boundary group, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Admin Scope**.	The IP IGMP Admin Scope window opens.
5. Select the name of the IGMP boundary group that you want to disable or reenable.	Your selection is highlighted.
6. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-84.	
7. Click on **Done**.	You return to the Configuration Manager window.

Configuring IGMP Policies

Site Manager allows you to create IGMP group policies and IGMP static forwarding entry policies.

For more information about groups, see “Multicast Host Groups” on page 1-2.

Configuring IGMP Group Policies

Use the following Site Manager procedure to create an IGMP group policy:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Policy Filters**.	The IP Policies menu opens.
4. Choose **IGMP**.	The IGMP Policies menu opens.
5. Choose **Group Policies**.	The IGMP Group Policy Filters window opens.
6. Click on **Add**.	The Add IGMP Group Policy Filter window opens.
7. Set the following parameters: • **Name** • **Sources** • **Action** • **Rule Precedence** • **Groups** • **Receivers’ Circuits** • **Receivers** Click on **Help** or see the parameter descriptions beginning on page A-76.	
8. Click on **OK**.	You return to the IGMP Group Policy Filters window.
9. Click on **Done**.	You return to the Configuration Manager window.

Disabling and Reenabling IGMP Group Policies

When you create an IGMP group policy, by default it is enabled.

To disable or reenable an IGMP group policy, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Policy Filters**.	The IP Policies menu opens.
4. Choose **IGMP**.	The IGMP Policies menu opens.
5. Choose **Group Policies**.	The IGMP Group Policy Filters window opens.
6. Select the name of the IGMP group policy that you want to disable or reenable.	Your selection is highlighted.
7. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-76.	
8. Click on **Done**.	You return to the Configuration Manager window.

Configuring IGMP Static Forwarding Policies

You configure IGMP static forwarding policies to forward multicast traffic as follows:

- Between multicast (*dynamic*) and nonmulticast (*static*) interfaces
- Into and out of nonmulticast interfaces

In Figure 3-1, multicast traffic is forwarded to a router that is configured with IGMP. To create an IGMP static forwarding policy for this type of scenario:

- Set the forwarding mode to static.
- Specify the in circuits (in this example, IGMP interface 1).
- Specify the out circuits (in this example, IGMP interfaces 2 and 3).

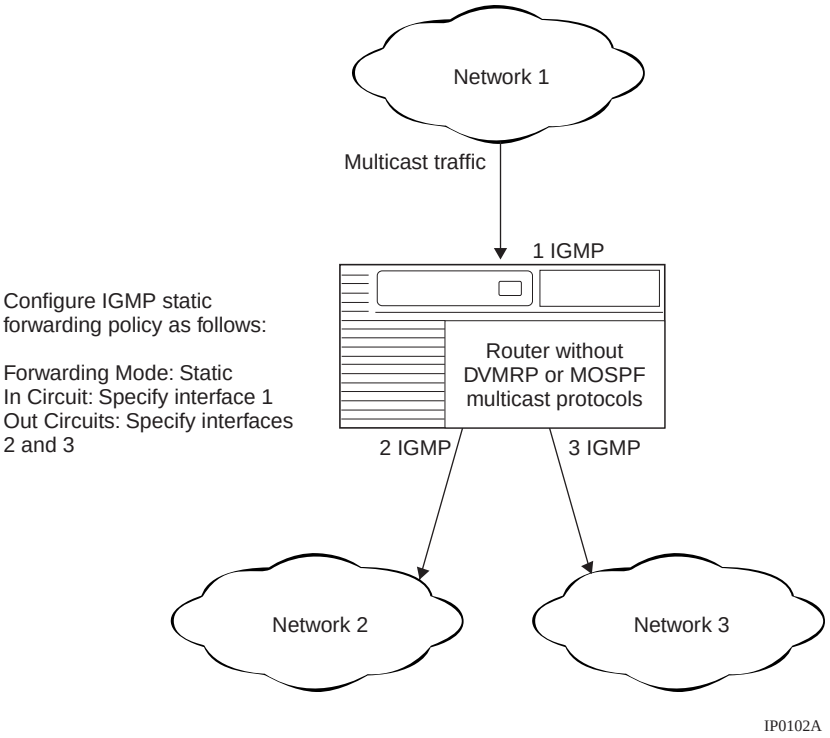

Figure 3-1. Forwarding Multicast Traffic over Static Interfaces

In Figure 3-2, multicast traffic is forwarded from a nonmulticast network to a nonmulticast interface on the router and is sent out through multicast interfaces on the same router. To create an IGMP static forwarding policy for this type of scenario:

- Set the forwarding mode to “static to dynamic.”
- Specify the in circuit (in this example, IGMP interface 1).
- Set the inbound IGMP circuit’s static forward cache lifetime to a value appropriate for the multicast protocol that will be transferring the traffic out of the router. For instructions, see “Specifying the Static Forward Cache Lifetime” on page 3-27.

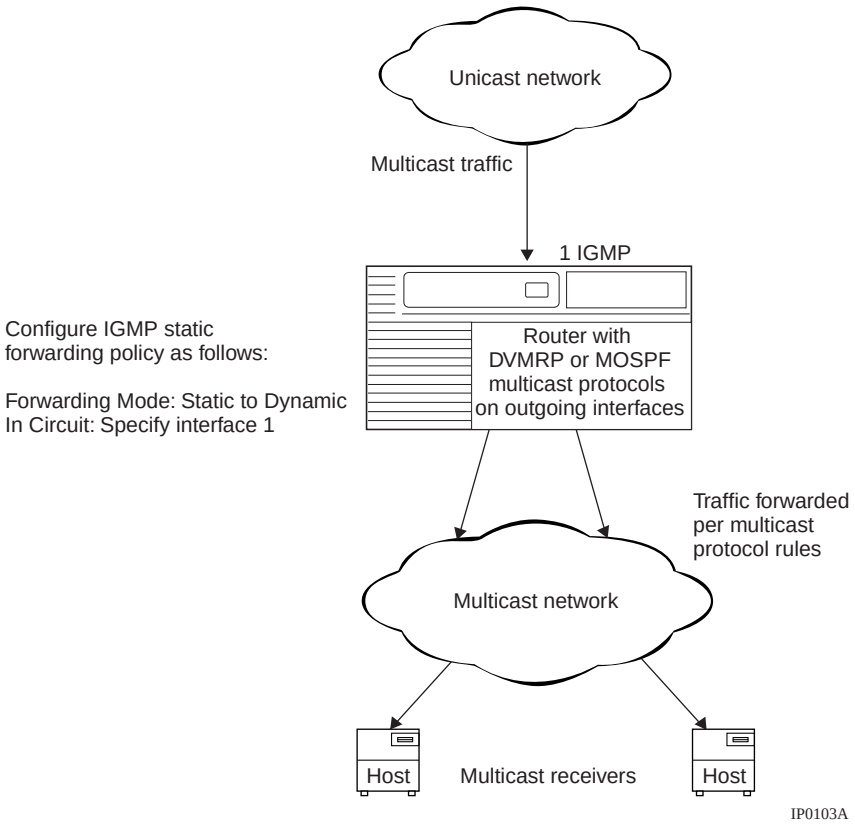

Figure 3-2. Forwarding Multicast Traffic from a Static Network to a Dynamic Network

In Figure 3-3, multicast traffic is forwarded to a multicast interface and on to nonmulticast interfaces. To create an IGMP static forwarding policy for this type of scenario:

- Set the forwarding mode to “dynamic to static.”
- Specify the static out circuits (in this example, IGMP interfaces 2 and 3).

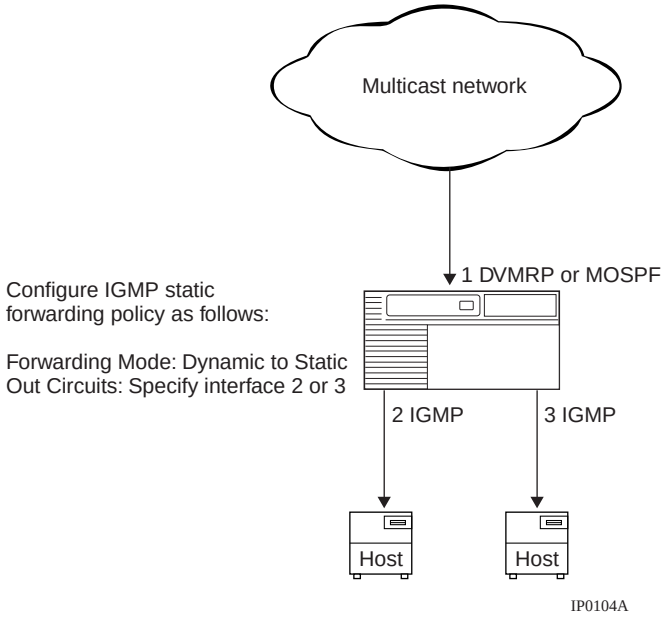

Figure 3-3. Forwarding Multicast Traffic from a Dynamic Network to Static Interfaces

For more information about multicast migration tools, see “Multicast Migration” on page 1-6.

To configure an IGMP static forwarding policy, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Policy Filters.**	The IP Policies menu opens.
4. Choose **IGMP.**	The IGMP Policies menu opens.
5. Choose **Static Forwarding Entries**.	The IGMP Static Forwarding Entries window opens.
6. Click on **Add**.	The Add IGMP Static Forwarding Entry window opens.
7. Set the following parameters: • **Name** • **Forwarding Mode** • **Rule Precedence** • **Groups** • **Sources** • **In Circuits** • **Out Circuits** Click on **Help** or see the parameter descriptions beginning on page A-80.	
8. Click on **OK**.	You return to the IGMP Static Forwarding Entries window.
9. Click on **Done**.	You return to the Configuration Manager window.

Disabling and Reenabling IGMP Static Forwarding Policies

When you create an IGMP static forwarding policy, by default it is enabled.

To disable or reenable an IGMP static forwarding policy, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Policy Filters**.	The IP Policies menu opens.
4. Choose **IGMP**.	The IGMP Policies menu opens.
5. Choose **Static Forwarding Entries**.	The IGMP Static Forwarding Entries window opens.
6. Select the name of the IGMP static forwarding policy that you want to disable or reenable.	Your selection is highlighted.
7. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-80.	
8. Click on **Done**.	You return to the Configuration Manager window.

Deleting IGMP

To delete IGMP from an IP interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a connector configured with IGMP.	The Edit Connector window opens.
2. Choose **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens.
5. Click on **IGMP/IGMP Relay**.	Site Manager deselects IGMP.
6. Click on **OK**.	You return to the Circuit Definition window.
7. Choose **File**.	The File menu opens.
8. Choose **Exit**.	You return to the Configuration Manager window.

Chapter 4
Customizing DVMRP

This chapter describes the Distance Vector Multicast Routing Protocol (DVMRP) and how to customize it on your router.

Topic	Page
DVMRP Concepts and Terminology	4-2
Customizing DVMRP Globally	4-8
Customizing DVMRP on an Interface	4-30
Configuring a DVMRP Tunnel	4-50
Configuring DVMRP Policies	4-69
Deleting DVMRP	4-84

DVMRP Concepts and Terminology

DVMRP is a multicasting protocol that provides a mechanism for routers to propagate multicast datagrams in a manner that minimizes the number of excess copies sent to any particular network.

This section covers the following topics:

Topic	Page
Neighbor Connections	4-2
Source Route Advertisements	4-4
How DVMRP Chooses a Route	4-5
Routing Table	4-6
Shortest-Path Trees	4-6
Tree Pruning	4-7

Neighbor Connections

In a DVMRP environment, *neighbors* are multicasting routers that are connected directly or through a tunnel:

- *Directly connected neighbors* are routers that have an interface to the same network.
- *Tunnel-connected neighbors* are multicast routers that communicate through a unicast network, exchanging DVMRP messages that are encapsulated in IP datagrams.

In Figure 4-1, for example, multicast router A has two neighbors, router B and router C. Router A and router B are connected directly -- they both have interfaces to net 6. Router A and router C communicate through a tunnel that includes a unicast router.

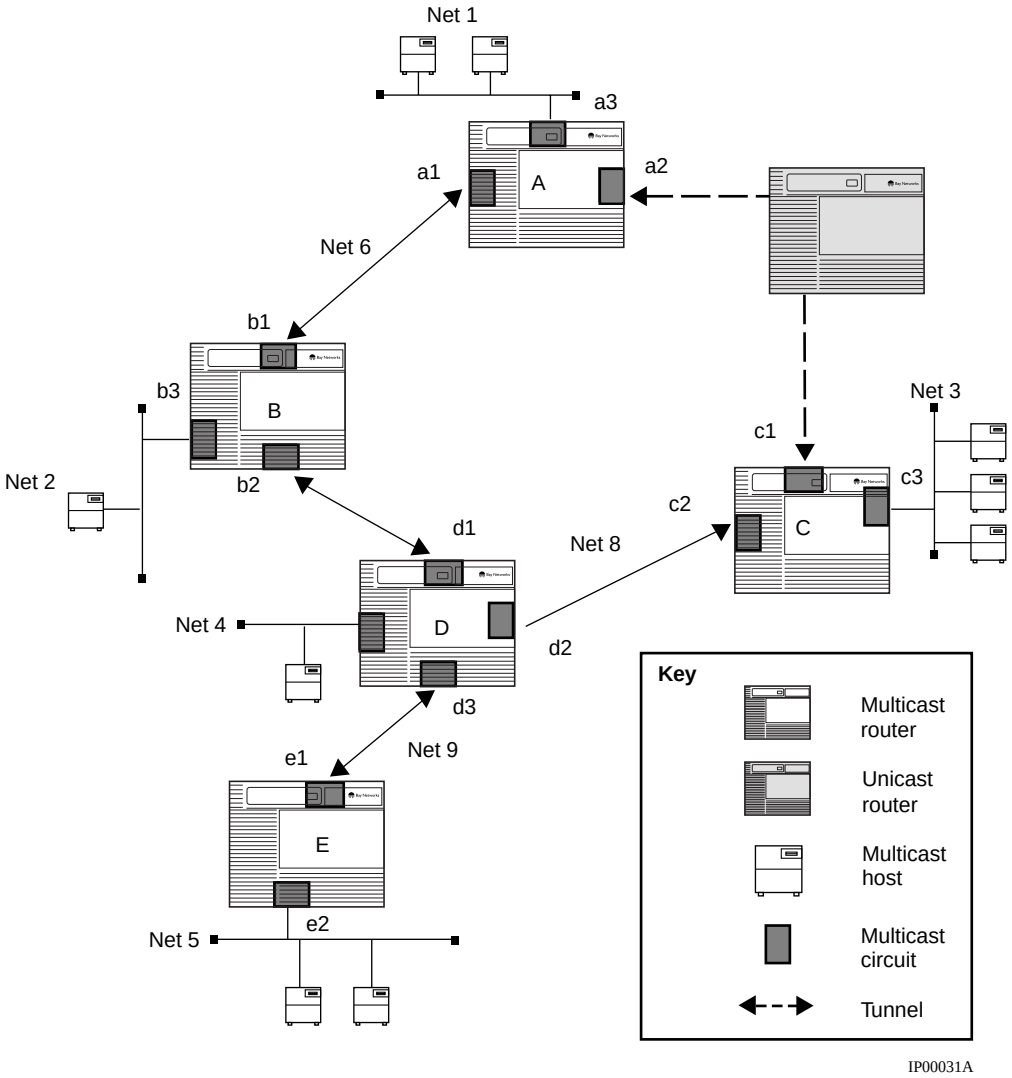

Figure 4-1. Multicast Routers

At startup, a DVMRP multicast router:

1. Initializes its routing table with information about all of its local networks
2. Learns the existence of its neighbors by sending a probe for all routes on each of its multicast interfaces
3. Receives reports from its neighbors containing the routing information (including route costs)

In Figure 4-1, for example, router D becomes active and issues routing probes on four multicasting interfaces. Router D receives reports from its multicasting neighbors, routers B, C, and E.

Source Route Advertisements

A *source network* is any network containing hosts that can issue multicast datagrams. DVMRP advertises shortest-path routes to multicasting source networks. In this respect, DVMRP is the opposite of RIP, which advertises routes to destination networks.

Periodically, each multicasting router issues full or partial routing information on each DVMRP interface, using DVMRP report messages. This routing information represents the sending router's cost to reach the specified source network. (The *cost* is the sum of the hop metrics along the shortest path to the given source network.)

Upon receiving a DVMRP report from another router, DVMRP reexamines its routing table to determine whether the shortest path information needs updating. Specifically, DVMRP looks in the routing table for an entry describing a route to the same source network. If one exists, DVMRP compares the cost of the two routes and stores the route with the lower cost in its routing table.

A router will not send route reports on an interface until it knows (by means of received probes or reports) that it has a neighboring multicast router on that interface. It will continue to send probes periodically on an interface.

How DVMRP Chooses a Route

Each DVMRP interface is configured with a metric that indicates the cost of the hop. A router that receives multiple route reports for the same multicasting source network:

- Compares the cost specified in each (based on the metric field)
- Stores information from the report with the lowest cost in its routing table

A *route metric* is the sum of all the interface (hop) metrics from a given route source to a given router.

In Figure 4-1 on page 4-3, for example, router D receives two reports for the network connected to multicast router A: one from router B and one from router C. Using the metrics contained in the route reports, router D determines that the cost of the tunneled route is greater than the cost of the route that uses direct physical connections. Router D discards the route received from router C and stores the route received from router B.

Router D then declares router B to be the next-hop neighbor and interface d1 to be the next-hop interface. After a next-hop neighbor has been declared for a route, the route updates received from that neighbor for that route take precedence until either the route times out or until another router advertises a better metric for that route.

Routing Table

Table 4-1 shows the principal items in a DVMRP routing table entry.

Table 4-1. DVMRP Routing Table Entry

Item	Description
Source subnet address and mask	Address and mask of a subnetwork containing a host sourcing multicast datagrams
From-gateway	Previous-hop router leading back to the source subnet
TTL	Number of seconds before this entry is removed from the routing table

Note that the source subnet and the previous-hop router in the DVMRP routing table are the opposite of the destination subnet and next-hop router in a RIP routing table.

Using this information, the router can:

1. Receive a multicast datagram and determine whether the datagram arrived on the interface that is on the shortest path to the source network.
2. Drop the datagram if it has not arrived on the shortest-path interface.
3. Flood the multicast datagram to all active downstream DVMRP neighbors.

Shortest-Path Trees

Route information used by DVMRP is independent of any other routing information used by the router -- for example, routes provided by RIP. The purpose of DVMRP routing information is to create a shortest-path tree entry in the routing table for the propagation of multicast datagrams.

The shortest-path tree entry indicates the interface that provides the shortest path to the network that is the source of the multicast datagram.

In Figure 4-1 on page 4-3, for example, the routing table on router D includes an entry describing the shortest-path route to the network connected to router A. The entry indicates that interface d1 provides the shortest path to that source network.

A shortest-path tree also indicates those interfaces that are on the shortest path to that source network from a neighboring router.

Router E considers the network connecting it to router D to be on the shortest path to the source network connected to router A. Router D has an interface (d3) that is part of the shortest path from router E to the network connected to router A.

If neighboring routers have the same metric to a given source network, the router with the lower IP address is responsible for propagating multicast traffic originating from that source network onto the network or tunnel that is common to these neighboring routers.

A network is considered a *leaf network* if it has no dependent downstream neighbors for a source. In Figure 4-1, the network connected to router E (net 5) is a leaf network.

Tree Pruning

If no members are detected on a branch of the shortest-path tree for a given group, DVMRP *prunes* the branch.

The following conditions cause DVMRP to prune the shortest-path tree for a given group:

- The router determines that the attached network on which the host is located (or any other locally attached network) has no active member of the group.
- The router determines that all neighbors on all attached networks other than the next-hop network to the source have pruned the source and group.
- The router determines that it is not located on the shortest network path to any remote network that includes a member of the group.

If any of these conditions are true, the router sends a DVMRP prune message to its DVMRP neighbor. The neighbor removes the router from its forwarding table.

If the host later rejoins the group, the router sends the neighbor a DVMRP graft message. The neighbor restores the router to its forwarding table.

Customizing DVMRP Globally

When you start DVMRP on the router, DVMRP runs with default values for all global parameters. You customize DVMRP by modifying parameters as described under the following topics:

Topic	Page
Disabling and Reenabling DVMRP Globally	4-9
Setting the Update Interval	4-10
Disabling and Reenabling Tree Pruning	4-12
Setting the Route Expiration Timer	4-13
Setting the Unconfirmed Route Timer	4-15
Setting the Neighbor Report Timer	4-17
Setting the Leaf Timer	4-19
Specifying a Probe Interval	4-21
Specifying a Route Switch Interval	4-23
Estimating the Number of Routes	4-25
Specifying the Maximum Number of Routes	4-27
Logging DVMRP Messages	4-29

Disabling and Reenabling DVMRP Globally

You can use the BCC or Site Manager to disable and reenable DVMRP globally on the router.

Using the BCC

To disable or reenable DVMRP on the router, navigate to the global DVMRP prompt (for example, **box; ip; dvmrp**) and enter:

state *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command disables DVMRP on the router:

```
dvmrp# state disabled
dvmrp#
```

Using Site Manager

To disable or reenable DVMRP, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Global**.	The DVMRP Global Configuration window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-2.	
6. Click on **Save**.	You return to the Configuration Manager window.

Setting the Update Interval

Periodically, each multicasting router issues full or partial routing information on each DVMRP interface, using DVMRP report messages. This routing information represents the sending router's cost to reach the specified network. (The *cost* is the sum of the hop metrics along the shortest path to the given source network.)

You can use the BCC or Site Manager to:

- Specify how often routing messages containing complete routing tables are sent.
- Specify the minimum amount of time between *triggered updates*. Triggered updates are sent when routing information changes. Issuing a full update restarts the triggered update timer. Therefore, the triggered update interval must be shorter than the full update interval.

Using the BCC

Specifying the Full Update Interval

To specify the full-update interval, navigate to the global DVMRP prompt (for example, **stack; ip; dvmrp**) and enter:

full-update-interval *<seconds>*

seconds is an integer representing the number of seconds in the interval. The default value is 60.

For example, the following command specifies a full-update interval of 120 seconds:

```
dvmrp# full-update-interval 120
dvmrp#
```

Specifying the Triggered Update Interval

To specify the triggered-update interval, navigate to the global DVMRP prompt and enter:

triggered-update-interval *<seconds>*

seconds is an integer representing the number of seconds in the interval. The default value is 5.

For example, the following command specifies a triggered-update interval of 10 seconds:

```
dvmrp# triggered-update-interval 10
dvmrp#
```

Using Site Manager

To set the full-update and triggered-update intervals, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Global**.	The DVMRP Global Configuration window opens.
5. Set the following parameters: • **Full Update Interval** • **Triggered Update Interval** Click on **Help** or see the parameter descriptions beginning on page A-3.	
6. Click on **Save**.	You return to the Configuration Manager window.

Disabling and Reenabling Tree Pruning

Tree pruning is enabled on the router by default. You can use the BCC or Site Manager to disable and reenable tree pruning on the router. For information about DVMRP tree pruning, see “Tree Pruning” on page 4-7.

Using the BCC

To disable or reenable tree pruning, navigate to the global DVMRP prompt (for example, **box; ip; dvmrp**) and enter:

pruning *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command disables DVMRP tree pruning on the router:

```
dvmrp# pruning disabled
dvmrp#
```

Using Site Manager

To disable or reenable tree pruning, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Global**.	The DVMRP Global Configuration window opens.
5. Set the **Pruning Enable** parameter. Click on **Help** or see the parameter description on page A-7.	
6. Click on **Save**.	You return to the Configuration Manager window.

Setting the Route Expiration Timer

The route expiration timer determines how long DVMRP waits for an update message indicating that a route is reachable. Upon expiration of this timer, this route is advertised as unreachable until it is refreshed or until it is deleted.

By default, DVMRP sets the route expiration timer to 200 seconds (3 minutes, 20 seconds). You can use the BCC or Site Manager to set the route expiration time from 20 through 4000 seconds (1 hour, 6 minutes, and 40 seconds).

Note: DVMRP timers must be the same throughout the network.

Using the BCC

To reset the route expiration timer, navigate to the global DVMRP prompt (for example, **box; ip; dvmrp**) and enter:

route-expiration-timeout *<seconds>*

seconds is an integer from 20 through 4000 indicating the number of seconds.

For example, the following command sets the route expiration timer to 500 seconds (8 minutes, 20 seconds):

```
dvmrp# route-expiration-timeout 500
dvmrp#
```

Using Site Manager

To set the route expiration timer, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Global**.	The DVMRP Global Configuration window opens.
5. Set the **Route Expiration Timeout** parameter. Click on **Help** or see the parameter description on page A-4.	
6. Click on **Save**.	You return to the Configuration Manager window.

Setting the Unconfirmed Route Timer

The unconfirmed route timer determines how long DVMRP advertises a route as unreachable before it removes the route from the routing table. The difference between this value and the route expiration timeout value represents the time period that the route will be advertised as unreachable without subsequent refreshment.

By default, DVMRP sets the unconfirmed route timer to 340 seconds (5 minutes, 40 seconds). You can use the BCC or Site Manager to set the value from 40 through 8000 seconds (2 hours, 13 minutes, and 20 seconds). Enter a value that is greater than the value you specified for the route expiration timer to allow enough time for the route to be advertised as unreachable.

Note: DVMRP timers must be the same throughout the network.

Using the BCC

To reset the unconfirmed route timer, navigate to the global DVMRP prompt (for example, **stack; ip; dvmrp**) and enter:

unconfirmed-route-timeout <*seconds*>

seconds is an integer from 40 through 8000 indicating the maximum number of seconds that DVMRP advertises an unreachable route.

For example, the following command sets the unconfirmed timer to 1000 seconds (16 minutes, 40 seconds):

```
dvmrp# unconfirmed-route-timeout 1000
dvmrp#
```

Using Site Manager

To set the unconfirmed route timer, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Global**.	The DVMRP Global Configuration window opens.
5. Set the **Garbage Timeout** parameter. Click on **Help** or see the parameter description on page A-5.	
6. Click on **Save**.	You return to the Configuration Manager window.

Setting the Neighbor Report Timer

The neighbor report timer specifies how long the router waits to receive a report from a neighbor before considering the connection inactive.

By default, DVMRP waits 140 seconds (2 minutes, 20 seconds). You can use the BCC or Site Manager to specify a value from 40 through 8000 seconds (2 hours, 13 minutes, and 20 seconds).

Note: DVMRP timers must be the same throughout the network.

Using the BCC

To reset the neighbor report timer, navigate to the global DVMRP prompt (for example, **box; ip; dvmrp**) and enter:

neighbor-timeout *<seconds>*

seconds is an integer from 40 through 8000 indicating the number of seconds.

For example, the following command sets the neighbor report timer to 150 seconds (2 minutes, 30 seconds):

```
dvmrp# neighbor-timeout 150
dvmrp#
```

Using Site Manager

To set the neighbor report timer, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Global**.	The DVMRP Global Configuration window opens.
5. Set the **Neighbor Timeout** parameter. Click on **Help** or see the parameter description on page A-4.	
6. Click on **Save**.	You return to the Configuration Manager window.

Setting the Leaf Timer

When DVMRP advertises a route on an interface, it waits a period of time for a DVMRP neighbor (that is, a multicast router) to respond positively. If no neighbor responds in the given time, the router considers the network attached to the interface to be a leaf network. The *leaf timer* allows you specify how long the router waits for a response from a neighbor.

The leaf timer determines whether or not a network (or tunnel) local to a given interface is considered to be part of the shortest path to a given source network by any DVMRP neighbor.

By default, DVMRP sets the leaf timer to 200 seconds (3 minutes, 20 seconds). You can use the BCC or Site Manager to specify a value from 25 through 4000 seconds (1 hour, 6 minutes, and 40 seconds).

Note: DVMRP timers must be the same throughout the network.

Using the BCC

To reset the leaf timer, navigate to the global DVMRP prompt (for example, **box; ip; dvmrp**) and enter:

leaf-timeout *<seconds>*

seconds is an integer from 25 through 4000 indicating the number of seconds.

For example, the following command sets the leaf timer to 250 seconds (4 minutes, 10 seconds):

```
dvmrp# leaf-timeout 250
dvmrp#
```

Using Site Manager

To set the leaf timer, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Global**.	The DVMRP Global Configuration window opens.
5. Set the **Leaf Timeout** parameter. Click on **Help** or see the parameter description on page A-3.	
6. Click on **Save**.	You return to the Configuration Manager window.

Specifying a Probe Interval

The probe interval determines how often DVMRP sends a probe on interfaces from which no neighbors have been heard.

By default, DVMRP sends a probe every 10 seconds. You can use the BCC or Site Manager to specify a value from 5 through 30 seconds.

If the neighbor is running DVMRP *mrouted*, ensure that your probe interval value matches the value used by the neighbor.

Using the BCC

To reset the probe interval, navigate to the global DVMRP prompt (for example, **box; ip; dvmrp**) and enter:

neighbor-probe-interval *<seconds>*

seconds is an integer from 5 through 30 indicating the number of seconds.

For example, the following command sets the DVMRP probe interval to 20 seconds:

```
dvmrp# neighbor-probe-interval 20
dvmrp#
```

Using Site Manager

To specify a probe interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Global**.	The DVMRP Global Configuration window opens.
5. Set the **Neighbor Probe Interval** parameter. Click on **Help** or see the parameter description on page A-6.	
6. Click on **Save**.	You return to the Configuration Manager window.

Specifying a Route Switch Interval

The route switch interval specifies how long the router should wait, without receiving a subsequent route update from the original neighbor, before switching to a different neighbor advertising equal cost for this route.

By default, DVMRP waits 140 seconds (2 minutes, 20 seconds). You can use the BCC or Site Manager to specify a value from 20 through 2000 seconds (33 minutes, 20 seconds).

If the neighbor is running DVMRP *mrouted*, you should accept the default value, 140 seconds.

Using the BCC

To reset the route switch interval, navigate to the global DVMRP prompt (for example, **box; ip; dvmrp**) and enter:

switch-timeout *<seconds>*

seconds is an integer from 20 through 2000 indicating the number of seconds.

For example, the following command sets the route switch interval to 120 seconds:

```
dvmrp# switch-timeout 120
dvmrp#
```

Using Site Manager

To specify the route switch interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Global**.	The DVMRP Global Configuration window opens.
5. Set the **Route Switch Timeout** parameter. Click on **Help** or see the parameter description on page A-6.	
6. Click on **Save**.	You return to the Configuration Manager window.

Estimating the Number of Routes

By default, DVMRP preallocates space for a routing table with 25 entries. You can use the BCC or Site Manager to specify the number of entries (10 or more). For an MBone (multicast backbone) implementation, a value of 3000 or higher is recommended.

Note that routes are kept on a per-source-network basis, independent of multicast groups. This number must include a route for every network that is local to an interface configured for multicasting. Exceeding this size during router operation will not cause an error, but may cause the router to consume more memory than required.

Using the BCC

To reset the number of entries in the routing table, navigate to the global DVMRP prompt (for example, **box; ip; dvmrp**) and enter:

estimated-routes *<route>*

route is an integer (10 or greater) indicating the estimated number of entries needed in the routing table.

For example, the following command causes DVMRP to preallocate space for a routing table with 50 entries:

```
dvmrp# estimated-routes 50
dvmrp#
```

Using Site Manager

To preallocate the estimated number of routes, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Global**.	The DVMRP Global Configuration window opens.
5. Set the **Estimated Routes** parameter. Click on **Help** or see the parameter description on page A-5.	
6. Click on **Save**.	You return to the Configuration Manager window.

Specifying the Maximum Number of Routes

By default, DVMRP stores all learned routes in the routing table. You can use the BCC or Site Manager to specify the number of routes that DVMRP can learn per slot. This parameter limits the number of routes that can be stored in the routing table.

If you specify a maximum number of routes, you must include a route for every local network that has an interface configured for multicasting.

Using the BCC

To specify the maximum number of routes stored in the routing table, navigate to the global DVMRP prompt (for example, **stack; ip; dvmrp**) and enter:

max-routes *<max>*

max is an integer indicating the maximum number of routes.

For example, the following command causes DVMRP to store in the routing table a maximum of 25 learned routes per slot.

```
dvmrp# max-routes 25
dvmrp#
```

Using Site Manager

To specify the maximum number of routes, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Global**.	The DVMRP Global Configuration window opens.
5. Set the **Max Routes** parameter. Click on **Help** or see the parameter description on page A-7.	
6. Click on **Save**.	You return to the Configuration Manager window.

Logging DVMRP Messages

By default, DVMRP does not log debugging messages. You can use the BCC or Site Manager to enable message logging and to specify the level of debug messages. Note, however, that you should specify a level only when directed by Customer Support personnel to investigate a problem.

Using the BCC

To log DVMRP debugging messages, navigate to the global DVMRP prompt (for example, **stack; ip; dvmrp**) and enter:

debug-log *<options>*

options is one of the legal values for the command (enter **debug-log ?** to display these values).

For example, the following command causes DVMRP to log all debugging messages:

```
dvmrp# debug-log all-options
dvmrp#
```

Using Site Manager

To log debugging messages, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Global**.	The DVMRP Global Configuration window opens.
5. Set the **Debug Level** parameter. Click on **Help** or see the parameter description on page A-6.	
6. Click on **Save**.	You return to the Configuration Manager window.

Customizing DVMRP on an Interface

You customize DVMRP on an interface by modifying DVMRP parameters as described under the following topics:

Topic	Page
Disabling and Reenabling DVMRP on an Interface	4-31
Enabling Multicast Migration Between DVMRP and Nonmulticast Interfaces	4-32
Disabling and Reenabling Multicast Support	4-33
Calculating the Cost of an Interface	4-35
Specifying a Threshold	4-37
Configuring a Forwarding Table	4-39
Disabling Advertisement of Local Networks	4-42
Advertising a Default Route	4-44
Listening for a Default Route	4-46
Accepting Reports from Standard DVMRP Neighbors Only	4-47
Specifying the Lifetime of a Prune Message	4-49

Disabling and Reenabling DVMRP on an Interface

By default, DVMRP is enabled on an interface. You can use the BCC or Site Manager to disable and reenable it.

Using the BCC

To disable or reenable DVMRP on an interface, navigate to a DVMRP interface prompt (for example, **box; ethernet/2/2; ip/2.3.4.5/255.255.255.0; dvmrp**) and enter:

state <*state*>

state is one of the following:

enabled (default)
disabled

For example, the following command disables DVMRP on IP interface 2.3.4.5:

```
dvmrp/2.3.4.5# state disabled
dvmrp/2.3.4.5#
```

Using Site Manager

To disable and reenable DVMRP on an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Circuit**.	The DVMRP Circuit Parameters window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-7.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Enabling Multicast Migration Between DVMRP and Nonmulticast Interfaces

You can enable the flow of multicast and nonmulticast packets between multicast and nonmulticast networks by using IP traffic filters and by setting IGMP static forwarding policies. Remember that IGMP must be configured on all DVMRP interfaces.

Receiving Nonmulticast Traffic and Forwarding As Multicast

If you configure an appropriate IP traffic filter, a router can receive unicast or broadcast traffic on a DVMRP configured interface. The IP traffic filter converts the unicast and broadcast packets to multicast before forwarding the traffic on an outbound interface running a multicast protocol.

For instructions on how to configure IP traffic filters, see *Configuring Traffic Filters and Protocol Prioritization.*

Receiving and Forwarding Multicast Traffic

If the multicast traffic is received on a DVMRP interface, then DVMRP can forward the packets on either:

- An outbound interface configured with a multicast protocol, such as DVMRP, based on the multicast protocol routing table and any enabled policies.
- A nonmulticast, IGMP static configured outbound interface. To send multicast packets out on a nonmulticast interface, you must set the IGMP static forwarding policy to “dynamic to static” mode for that interface.

If the multicast traffic is received on a nonmulticast, static configured interface, set the IGMP static forwarding policy to “static to dynamic” mode and specify the static incoming interface to receive the traffic. You will also need to configure a DVMRP unicast accept policy with the appropriate network address information to inject into the DVMRP routing table.

To configure an IGMP static forwarding policy, see “Configuring IGMP Static Forwarding Policies” on page 3-33.

To configure a DVMRP unicast accept policy, see “Configuring DVMRP Unicast Accept Route Policies” on page 4-69.

Disabling and Reenabling Multicast Support

By default, DVMRP does the following:

- Propagates multicast routing information on the interface
- Incorporates in routing updates information about the source network associated with this interface
- Forwards multicast datagrams on this interface in *native mode* -- that is, as multicast datagrams

Using the BCC or Site Manager, you can disable multicast support on the interface.

Using the BCC

To disable or reenable multicast support, navigate to a DVMRP interface prompt (for example, **box; ethernet/2/2; ip/2.3.4.5/255.255.255.0; dvmrp**) and enter:

routing *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command disables DVMRP multicast routing on IP interface 2.3.4.5:

```
dvmrp/2.3.4.5# routing disabled
dvmrp/2.3.4.5#
```

Using Site Manager

To disable and reenable multicast support, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Circuit**.	The DVMRP Circuit Parameters window opens.
5. Set the **Route Enable** parameter. Click on **Help** or see the parameter description on page A-8.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Calculating the Cost of an Interface

By default, an interface has a cost of 1. Bay Networks recommends the values specified in Table 4-2.

Table 4-2. Recommended Costs for DVMRP Interfaces

Hop	Cost
LAN, or tunnel across a single LAN	1
Multihop tunnel	2 or 3
Serial link, or tunnel across a serial link	1
Backup tunnel	Primary tunnel metric + 1

You can use the BCC or Site Manager to assign a cost from 1 through 31.

Using the BCC

To specify the cost of an interface, navigate to a DVMRP interface prompt (for example, **box; ethernet/2/2; ip/2.3.4.5/255.255.255.0; dvmrp**) and enter:

metric *<metric>*

metric is an integer from 1 (the default) through 31 indicating the cost of the interface.

For example, the following command assigns a cost of 12 to DVMRP interface 2.3.4.5:

```
dvmrp/2.3.4.5# metric 12
dvmrp/2.3.4.5#
```

Using Site Manager

To specify the cost of an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Circuit**.	The DVMRP Circuit Parameters window opens.
5. Set the **Metric** parameter. Click on **Help** or see the parameter description on page A-8.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying a Threshold

Threshold values control the scope of datagram delivery. The threshold is the minimum IP TTL (in hops) required for a multicast datagram to be forwarded out a given interface.

For *mrouted* compatibility, multicast datagrams originated by the router have a TTL of 1. These datagrams are not compared against the TTL. Unicast datagrams originated by the router (for example, for route reports issued via a tunnel) have a TTL of 255. A datagram that is to be forwarded through a tunnel is first compared against the threshold and, if accepted, is then encapsulated in an IP datagram with a TTL of 64.

Table 4-3 lists:

- Originating TTL values recommended for certain types of multicast applications
- Threshold values recommended for routers to permit the forwarding of packets from these applications

These values are recommended for topologies that will connect to the MBone.

Table 4-3. Recommended TTL and Threshold Values

Multicast Application	TTL	Threshold
IETF channel 1 low-rate GSM audio	255	224
IETF channel 2 low-rate GSM audio	223	192
IETF channel 1 PCM audio	191	160
IETF channel 2 PCM audio	159	128
IETF channel 1 video	127	96
IETF channel 2 video	95	64
Local event audio	63	32
Local event video	31	1

By default, DVMRP uses a threshold value of 1. You can use the BCC or Site Manager to specify a TTL value from 1 through 254.

Using the BCC

To specify a threshold, navigate to a DVMRP interface prompt (for example, **box; ethernet/2/2; ip/2.3.4.5/255.255.255.0; dvmrp**) and enter:

ttl-threshold *<ttl>*

ttl is an integer from 1 (the default) through 254.

For example, the following command assigns a threshold value of 15 to DVMRP interface 2.3.4.5:

```
dvmrp/2.3.4.5# ttl-threshold 15
dvmrp/2.3.4.5#
```

Using Site Manager

To specify a threshold, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Circuit**.	The DVMRP Circuit Parameters window opens.
5. Set the **Threshold** parameter. Click on **Help** or see the parameter description on page A-9.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Configuring a Forwarding Table

To minimize the amount of time that it spends looking up routes, DVMRP creates and maintains a cache of frequently used routes -- called a *forwarding table* -- for each IP interface.

By default, DVMRP preallocates a forwarding table of 32 entries for each interface. You can specify the maximum number of entries (32 through 512) allowed in the forwarding table associated with this interface.

When configuring a forwarding cache size, you must also keep in mind the TTL value for entries. If you specify a large cache size, you can specify a larger TTL value. A smaller cache requires a smaller TTL for cache entries.

By default, DVMRP uses a TTL of 7200 seconds (2 hours) for entries in the forwarding table. You can specify a TTL from 300 seconds (5 minutes) through 86,400 seconds (24 hours).

If the neighbor is running *mrouted*, the recommended TTL value is 300 seconds.

Specifying the Maximum Number of Table Entries

To specify the maximum number of table entries, you can use the BCC or Site Manager.

Using the BCC

To specify the maximum number of entries allowed in the forwarding table on this interface, navigate to a DVMRP interface prompt (for example, **box; ethernet/2/2; ip/2.3.4.5/255.255.255.0; dvmrp**) and enter:

max-cache-size *<entries>*

entries is an integer indicating the number of entries preallocated for the forwarding table.

For example, the following command causes DVMRP to preallocate space for a forwarding table with 35 entries:

```
dvmrp/2.3.4.5# max-cache-size 35
dvmrp/2.3.4.5#
```

Using Site Manager

To specify the number of entries allowed in the forwarding table, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Circuit**.	The DVMRP Circuit Parameters window opens.
5. Set the **Forward Cache Size** parameter. Click on **Help** or see the parameter description on page A-9.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying a TTL for Forwarding Table Entries

To specify the timeout for cache entries in the forwarding table, you can use the BCC or Site Manager.

Using the BCC

To specify a TTL for entries in the forwarding table, navigate to a DVMRP interface prompt (for example, **box; ethernet/2/2; ip/2.3.4.5/255.255.255.0; dvmrp**) and enter:

fwd-cache-timeout *<seconds>*

seconds is an integer indicating the TTL of a forwarding table entry in seconds.

For example, the following command causes DVMRP to assign a TTL of 5000 seconds (1 hour, 23 minutes, and 20 seconds) to entries in the forwarding table on this interface:

```
dvmrp/2.3.4.5# fwd-cache-timeout 5000
dvmrp/2.3.4.5#
```

Using Site Manager

To specify a TTL for entries in the forwarding table, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Circuit**.	The DVMRP Circuit Parameters window opens.
5. Set the **Forward Cache TTL** parameter. Click on **Help** or see the parameter description on page A-9.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Disabling Advertisement of Local Networks

By default, DVMRP advertises its own local networks over this interface. Using the BCC or Site Manager, you can configure DVMRP so that it does not advertise local networks over the interface.

Using the BCC

To disable the advertisement of local networks, navigate to a DVMRP interface prompt (for example, **box; ethernet/2/2; ip/2.3.4.5/255.255.255.0; dvmrp**) and enter:

advertise-self *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command prevents DVMRP from advertising routes to its own local networks over IP interface 2.3.4.5:

```
dvmrp/2.3.4.5# advertise-self disabled
dvmrp/2.3.4.5#
```

Using Site Manager

To disable the advertisement of local networks, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Circuit**.	The DVMRP Circuit Parameters window opens.
5. Set the **Advertise Self** parameter. Click on **Help** or see the parameter description on page A-10.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Advertising a Default Route

By default, DVMRP advertises a default route on this router, if one exists in the DVMRP routing table. You can use the BCC or Site Manager to disable or reenable the advertising of the default route, or to generate a default route, as required.

Using the BCC

To disable or reenable the advertisement of a default route, or to enable the router to generate one, navigate to a DVMRP interface prompt (for example, **box; ethernet/2/2; ip/2.3.4.5/255.255.255.0; dvmrp**) and enter:

default-supply *<state>*

state is one of the following:

enabled (default)
disabled
generate

For example, the following command causes DVMRP to generate a default route over IP interface 2.3.4.5:

```
dvmrp/2.3.4.5# default-supply generate
dvmrp/2.3.4.5#
```

Using Site Manager

To disable or reenable the advertisement of a default route, or to enable the router to generate one, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Circuit**.	The DVMRP Circuit Parameters window opens.
5. Set the **Supply Default Route** parameter. Click on **Help** or see the parameter description on page A-10.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Listening for a Default Route

By default, DVMRP listens for a default route on this interface. You can use the BCC or Site Manager to enable and disable this feature as required.

Using the BCC

To prevent DVMRP from listening for a default route, or to reenable such listening, navigate to a DVMRP interface prompt (for example, **box; ethernet/2/2; ip/2.3.4.5/255.255.255.0; dvmrp**) and enter:

default-listen *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command causes DVMRP to stop listening for a default route over IP interface 2.3.4.5:

```
dvmrp/2.3.4.5# default-listen disabled
dvmrp/2.3.4.5#
```

Using Site Manager

To listen for a default route, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Circuit**.	The DVMRP Circuit Parameters window opens.
5. Set the **Listen Default Route** parameter. Click on **Help** or see the parameter description on page A-10.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Accepting Reports from Standard DVMRP Neighbors Only

A standard DVMRP router sends a probe message to a neighbor before it advertises a route report. DVMRP uses the probe message to learn the neighbor's capability. Some routers, however, send only route reports; they do not send probes. By default, DVMRP accepts reports from standard and nonstandard DVMRP neighbors.

You can use the BCC or Site Manager to allow a DVMRP interface to communicate with standard DVMRP routers only.

Using the BCC

To specify whether a DVMRP interface communicates with standard DVMRP routers only, navigate to a DVMRP interface prompt (for example, **box; ethernet/2/2; ip/2.3.4.5/255.255.255.0; dvmrp**) and enter:

depend-on-probe *<state>*

state is one of the following:

enabled
disabled (default)

For example, the following command configures DVMRP to communicate with standard DVMRP routers only on IP interface 2.3.4.5:

```
dvmrp/2.3.4.5# depend-on-probe enabled
dvmrp/2.3.4.5#
```

Using Site Manager

To specify whether a DVMRP interface accepts reports from standard DVMRP neighbors only, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Circuit**.	The DVMRP Circuit Parameters window opens.
5. Set the **Report Depend Probe** parameter. Click on **Help** or see the parameter description on page A-11.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying the Lifetime of a Prune Message

By default, a prune message that DVMRP sends to a neighbor on this interface has a lifetime of 7200 seconds (2 hours).

You can use the BCC or Site Manager to specify a lifetime value from 0 through 86,400 seconds (24 hours).

Using the BCC

To reset the lifetime of a prune message, navigate to a DVMRP interface prompt (for example, **box; ethernet/2/2; ip/2.3.4.5/255.255.255.0; dvmrp**) and enter:

prune-lifetime <*seconds*>

seconds is the lifetime of the prune message in seconds.

For example, the following command sets the lifetime value to 5000 seconds (1 hour, 23 minutes, and 20 seconds) for prune messages that DVMRP sends on IP interface 2.2.2.2:

```
dvmrp/2.2.2.2# prune-lifetime 5000
dvmrp/2.2.2.2#
```

Using Site Manager

To specify the lifetime of a prune message, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Circuit**.	The DVMRP Circuit Parameters window opens.
5. Set the **Prune Life Time** parameter. Click on **Help** or see the parameter description on page A-11.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Configuring a DVMRP Tunnel

You configure a DVMRP tunnel by setting parameters as described under the following topics:

Topic	Page
Supplying Addresses	4-51
Disabling and Reenabling a DVMRP Tunnel	4-53
Specifying the Encapsulation Mode for Tunneled Datagrams	4-54
Specifying the Cost	4-56
Specifying a Threshold	4-57
Configuring a Forwarding Table	4-59
Advertising a Default Route	4-62
Listening for a Default Route	4-64
Specifying an Encapsulation Mode for Control Messages	4-65
Accepting Reports from Standard DVMRP Neighbors Only	4-66
Specifying the Lifetime of a Prune Message	4-68

Supplying Addresses

To identify a unicast tunnel, you must supply the unicast IP address of each end of the tunnel: the local interface and the remote interface. You can use the BCC or Site Manager to supply these addresses.

Using the BCC

To supply addresses for a tunnel, navigate to the root prompt (box# or stack#) and enter:

tunnels

The tunnels prompt appears. Enter the following command:

dvmrp local *<local_ip_address>* **remote** *<remote_ip_address>*

local_ip_address is the unicast IP address of an interface on this router.

remote_ip_address is the unicast IP address of an interface on the remote DVMRP router.

For example, the following command configures a DVMRP unicast tunnel. The local end point of the tunnel is unicast IP interface 2.2.2.2. The remote end point of the tunnel is unicast IP interface 2.2.4.5.

```
box# tunnels
tunnels# dvmrp local 2.2.2.2 remote 2.2.4.5
dvmrp/2.2.2.2/2.2.4.5#
```

Using Site Manager

To supply addresses for a tunnel, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Tunnel**.	The DVMRP Tunnel Parameters window opens.
5. Click on **Add**.	The DVMRP Tunnel Address window opens.
6. Set the following parameters: • **Local IP Address** • **Remote IP Address** Click on **Help** or see the parameter descriptions beginning on page A-16.	
7. Click on **OK**.	You return to the DVMRP Tunnel Parameters window.

Disabling and Reenabling a DVMRP Tunnel

When you configure a DVMRP tunnel on an interface, the tunnel is enabled by default. You can use the BCC or Site Manager to disable and reenable the tunnel.

Using the BCC

To disable or reenable a tunnel, navigate to a DVMRP tunnel prompt (for example, **box; tunnels; dvmrp/2.2.2.2/2.2.4.5**) and enter:

state *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command disables DVMRP tunnel 2.3.4.5/4.4.2.3:

```
dvmrp/2.3.4.5/4.4.2.3# state disabled
dvmrp/2.3.4.5/4.4.2.3#
```

Using Site Manager

To disable and reenable a DVMRP tunnel, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Tunnel**.	The DVMRP Tunnel Parameters window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-12.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying the Encapsulation Mode for Tunneled Datagrams

By default, DVMRP encapsulates a tunneled multicast datagram in an IP unicast datagram. Using the BCC or Site Manager, you can configure DVMRP to loosely encapsulate multicast datagrams using the LSSR option. See RFC 1075 for information about the LSSR option, which is provided for backward compatibility.

Using the BCC

To reset the encapsulation mode, navigate to a DVMRP tunnel prompt (for example, **box; tunnels; dvmrp/2.2.2.2/2.2.4.5**) and enter:

data-encapsulation *<mode>*

mode is one of the following:

ip-in-ip (default)
lssr

For example, the following command specifies LSSR encapsulation for the tunnel:

```
dvmrp/2.3.4.5/4.4.2.3# data-encapsulation lssr
dvmrp/2.3.4.5/4.4.2.3#
```

Using Site Manager

To choose an encapsulation mode, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Tunnel**.	The DVMRP Tunnel Parameters window opens.
5. Set the **Encapsulation Mode** parameter. Click on **Help** or see the parameter description on page A-12.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying the Cost

By default, DVMRP assigns a cost metric of 1 to a tunnel (for recommended values, see Table 4-2 on page 4-35). You can use the BCC or Site Manager to specify a cost value from 1 through 31.

Using the BCC

To specify the cost of a tunnel, navigate to a DVMRP tunnel prompt (for example, **box; tunnels; dvmrp/2.2.2.2/2.2.4.5**) and enter:

metric *<metric>*

metric is an integer from 1 (the default) through 31.

For example, the following command assigns a cost of 15 to DVMRP tunnel 2.3.4.5/4.4.2.3:

```
dvmrp/2.3.4.5/4.4.2.3# metric 15
dvmrp/2.3.4.5/4.4.2.3#
```

Using Site Manager

To specify the cost metric of a tunnel, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Tunnel**.	The DVMRP Tunnel Parameters window opens.
5. Set the **Metric** parameter. Click on **Help** or see the parameter description on page A-12.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying a Threshold

By default, DVMRP assigns a threshold value of 1 to a tunnel. This value is the minimum IP TTL required for a multicast datagram to be forwarded out this tunnel. You can use the BCC or Site Manager to assign a value from 1 through 254.

Use this value to control the scope of the datagrams. If the IP TTL is less than the threshold value you specify, the router drops the datagram.

Using the BCC

To specify a threshold value, navigate to a DVMRP tunnel prompt (for example, **box; tunnels; dvmrp/2.2.2.2/2.2.4.5**) and enter:

threshold *<ttl>*

ttl is an integer from 1 (the default) through 254.

For example, the following command assigns a threshold TTL value of 15 to DVMRP tunnel 2.3.4.5/4.4.2.3:

```
dvmrp/2.3.4.5/4.4.2.3# threshold 15
dvmrp/2.3.4.5/4.4.2.3#
```

Using Site Manager

To specify a threshold value, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Tunnel**.	The DVMRP Tunnel Parameters window opens.
5. Set the **Threshold** parameter. Click on **Help** or see the parameter description on page A-13.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Configuring a Forwarding Table

By default, DVMRP preallocates a forwarding table -- or cache -- for 32 entries. You can use the BCC or Site Manager to specify the maximum number of entries (from 32 through 512) allowed in the forwarding table associated with this tunnel interface.

When configuring a cache size, you must also keep in mind the TTL value for entries. If you specify a large cache size, you can specify a larger TTL value. A smaller cache requires a smaller TTL for cache entries.

By default, DVMRP assigns a TTL value of 7200 seconds (2 hours) to an entry in a tunnel forwarding table. You can use the BCC or Site Manager to assign a value from 300 seconds (5 minutes) through 86,400 seconds (24 hours).

Specifying the Forwarding Table Size

To specify the forwarding table size, you can use the BCC or Site Manager.

Using the BCC

To specify the size of the forwarding table for a tunnel, navigate to a tunnel prompt (for example, **box; tunnels; dvmrp/2.2.2.2/2.2.4.5**) and enter:

cache-size <*entries*>

entries is the number of entries that DVMRP preallocates for the forwarding table. The default value is 32 entries.

For example, the following command causes DVMRP to preallocate space for a forwarding table with 50 entries for tunnel 2.3.4.5/4.4.2.3:

```
dvmrp/2.3.4.5/4.4.2.3# cache-size 50
dvmrp/2.3.4.5/4.4.2.3#
```

Using Site Manager

To configure a cache size for the forwarding table, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Tunnel**.	The DVMRP Tunnel Parameters window opens.
5. Set the **Forward Cache Size** parameter. Click on **Help** or see the parameter description on page A-13.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying the Timeout for Cache Entries

To specify the timeout for cache entries in the forwarding table, you can use the BCC or Site Manager.

Using the BCC

To specify a timeout value for entries in the cache, navigate to a tunnel prompt (for example, **box; tunnels; dvmrp/2.2.2.2/2.2.4.5**) and enter:

cache-timeout <*seconds*>

seconds is the timeout value in seconds. The default value is 7200 seconds.

For example, the following commands cause DVMRP to preallocate a forwarding table for 50 entries for tunnel 3.3.3.3/3.3.3.4. The timeout value for entries in this table is 8000 seconds (2 hours, 13 minutes, and 20 seconds).

```
dvmrp/3.3.3.3/3.3.3.4# cache-size 50
dvmrp/3.3.3.3/3.3.3.4# cache-timeout 8000
dvmrp/3.3.3.3/3.3.3.4#
```

Using Site Manager

To specify the cache TTL for the table entries, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Tunnel**.	The DVMRP Tunnel Parameters window opens.
5. Set the **Forward Cache TTL (Secs)** parameter. Click on **Help** or see the parameter description on page A-13.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Advertising a Default Route

By default, DVMRP advertises a default route on this tunnel, if one exists in the DVMRP routing table. You can use the BCC or Site Manager to disable or reenable the advertising of a default route, or to generate a default route, as required.

Using the BCC

To disable or reenable the advertisement of a default route, or to enable the router to generate one, navigate to a DVMRP tunnel prompt (for example, **box; tunnels; dvmrp/2.2.2.2/2.2.4.5**) and enter:

default-supply *<state>*

state is one of the following:

enabled (default)
disabled
generate

For example, the following command causes DVMRP to generate a default route on tunnel 2.2.2.2/4.4.3.2:

```
dvmrp/2.2.2.2/4.4.3.2# default-supply generate
dvmrp/2.2.2.2/4.4.3.2#
```

Using Site Manager

To disable or reenable the advertisement of a default route, or to enable the router to generate one, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Tunnel**.	The DVMRP Tunnel Parameters window opens.
5. Set the **Route Supply** parameter. Click on **Help** or see the parameter description on page A-14.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Listening for a Default Route

By default, DVMRP listens for a default route on this tunnel. You can use the BCC or Site Manager to disable or reenable this feature as required.

Using the BCC

To prevent a DVMRP tunnel from listening for a default route, or to reenable such listening, navigate to a DVMRP tunnel prompt (for example, **box; tunnels; dvmrp/2.2.2.2/2.2.4.5**) and enter:

default-listen *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command configures DVMRP to stop listening for a default route on tunnel 2.2.2.2/4.4.3.2:

```
tunnel/2.2.2.2/4.4.3.2# default-listen disabled
tunnel/2.2.2.2/4.4.3.2#
```

Using Site Manager

To listen for a default route, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Tunnel**.	The DVMRP Tunnel Parameters window opens.
5. Set the **Route Listen** parameter. Click on **Help** or see the parameter description on page A-14.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying an Encapsulation Mode for Control Messages

To maintain backward compatibility with earlier versions of DVMRP, you can configure the encapsulation mode for DVMRP control packets.

Using the BCC

To reset the encapsulation mode for control packets, navigate to a DVMRP tunnel prompt (for example, **box; tunnels; dvmrp/2.2.2.2/2.2.4.5**) and enter:

control-encapsulation *<type>*

type is one of the following:

native (default)
ip-in-ip

For example, the following command specifies IP-in-IP control encapsulation for tunnel 2.2.2.2/4.4.3.2:

```
tunnel/2.2.2.2/4.4.3.2# control-encapsulation ip-in-ip
tunnel/2.2.2.2/4.4.3.2#
```

Using Site Manager

To specify an encapsulation mode for control messages, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Tunnel**.	The DVMRP Tunnel Parameters window opens.
5. Set the **Control Message Mode** parameter. Click on **Help** or see the parameter description on page A-14.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Accepting Reports from Standard DVMRP Neighbors Only

A standard DVMRP router sends a probe message to a neighbor before it advertises a route report. DVMRP uses the probe message to learn the neighbor's capability. Some routers, however, send only route reports; they do not send probes. By default, DVMRP accepts reports from standard and nonstandard DVMRP neighbors.

You can use the BCC or Site Manager to allow a DVMRP tunnel to communicate with standard DVMRP routers only.

Using the BCC

To specify whether a DVMRP tunnel communicates with standard DVMRP routers only, navigate to a DVMRP tunnel prompt (for example, **box; tunnels; dvmrp/2.2.2.2/2.2.4.5**) and enter:

depend-on-probe *<state>*

state is one of the following:

enabled
disabled (default)

For example, the following command configures DVMRP to communicate with standard DVMRP neighbors only on tunnel 2.2.2.2/4.4.3.2:

```
tunnel/2.2.2.2/4.4.3.2# depend-on-probe enabled
tunnel/2.2.2.2/4.4.3.2#
```

Using Site Manager

To specify whether a DVMRP tunnel accepts reports from standard DVMRP neighbors only, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Tunnel**.	The DVMRP Tunnel Parameters window opens.
5. Set the **Report Depend Probe** parameter. Click on **Help** or see the parameter description on page A-15.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying the Lifetime of a Prune Message

By default, a prune message that DVMRP sends to a neighbor on this tunnel has a lifetime of 7200 seconds (2 hours).

You can use the BCC or Site Manager to specify a lifetime value from 0 through 86,400 seconds (24 hours).

Using the BCC

To reset the lifetime of a prune message, navigate to a DVMRP tunnel prompt (for example, **box; tunnels; dvmrp/2.2.2.2/2.2.4.5**) and enter:

prune-lifetime <*seconds*>

seconds is the lifetime of the prune message in seconds.

For example, the following command sets the lifetime value to 5000 seconds (1 hour, 23 minutes, and 20 seconds) for prune messages that DVMRP sends on tunnel 2.2.2.2/2.2.2.4:

```
dvmrp/2.2.2.2/2.2.2.4# prune-lifetime 5000
dvmrp/2.2.2.2/2.2.2.4#
```

Using Site Manager

To specify the lifetime of a prune message, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DVMRP**.	The DVMRP menu opens.
4. Choose **Tunnel**.	The DVMRP Tunnel Parameters window opens.
5. Set the **Prune Life Time** parameter. Click on **Help** or see the parameter description on page A-15.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Configuring DVMRP Policies

The following topics describe how to configure DVMRP policies:

Topic	Page
Configuring DVMRP Unicast Accept Route Policies	4-69
Disabling or Reenabling DVMRP Unicast Accept Policies	4-73
Configuring DVMRP Accept Policies	4-74
Disabling or Reenabling DVMRP Accept Policies	4-78
Configuring DVMRP Announce Policies	4-79
Disabling or Reenabling DVMRP Announce Policies	4-83

Configuring DVMRP Unicast Accept Route Policies

A unicast accept route policy causes DVMRP to copy the routes you specify from the IP unicast routing table and inject them into the DVMRP routing table.

You must configure a DVMRP unicast accept policy to:

- Accept and forward multicast packets from a static configured nonmulticast network. For more information, see “Multicast Migration” on page 1-6.
- Connect a DVMRP router to an IGMP Relay device. For complete information, see “Configuring a DVMRP Router for Use with IGMP Relay” on page 9-20.

Before you can create a unicast accept policy on an interface, IGMP and DVMRP must be configured on the interface.

Using the BCC

To create a DVMRP unicast accept policy, navigate to the global DVMRP prompt (for example, **box; ip; dvmrp**) and enter:

unicast-accept *<polname>*

<polname> is the name of the DVMRP unicast accept policy.

For example, the following command creates a DVMRP unicast accept policy named “dvmrppol3”:

```
dvmrp# unicast-accept dvmrppol3
unicast-accept/dvmrppol3/dvmrp#
```

To customize a DVMRP unicast accept policy, set one or more of the following parameters (Table 4-4):

Table 4-4. DVMRP Unicast Accept Policy BCC Parameters

Parameter	Values (d = default)	Description
action	accept (d) | ignore	Specifies whether to accept or ignore the interfaces or networks for a route that matches this policy. • To import the matching route from the IP unicast routing table to the DVMRP routing table, specify accept. • If you do not want to import the matching route, specify ignore.
inject	null (d) | *list of IP addresses and masks*	Specifies a list of IP networks that DVMRP injects into the DVMRP routing table in place of the advertised networks. This parameter has meaning only if the action is set to accept. To inject the advertised network, use the default, null. Use this parameter to insert an aggregate or default network along with the actual network.
interface	null (d) | *IP address*	To apply the DVMRP unicast accept policy to advertisements that arrive on any interface, use the default, null. Otherwise, this parameter specifies the IP address of an interface that can receive DVMRP unicast updates to accept or ignore.
metric	1 (d) through 31	Specifies the cost of the route that DVMRP injects into the DVMRP routing table
network	*address mask* match exact | match range	Specifies the networks that match this policy, and whether you want the match to be exact or a range. • **match exact** means match the specific network advertisement (number and mask). • **match range** means match any network number that falls in the range indicated by the IP address and mask.
precedence	0 (d) through 2,147,483,647	Specifies a metric that DVMRP uses to compare this policy to other policies that match the route. DVMRP uses the precedence value to choose among multiple matches. In ranking policies according to precedence, keep in mind that the route with the highest value is the preferred route. In case of a tie, the most recent route wins.

(continued)

Table 4-4. DVMRP Unicast Accept Policy BCC Parameters *(continued)*

Parameter	Values (d = default)	Description
preference	0 (d) through 16	Specifies a value that DVMRP uses to compare the injected route to an existing route in the DVMRP routing table, higher preferred. This parameter has meaning only if the action is set to accept. If the injected unicast route is preferred, set the preference to a higher number than the value of the existing route. A route learned from a DVMRP network always has a preference of 1.
type	best route (d) | OSPF | both	Specifies whether the route used is best-route, OSPF, or both.

Examples

To specify a network address that must match the DVMRP policy, navigate to the DVMRP unicast accept policy prompt and enter the following commands:

```
unicast-accept/dvmrppol2/dvmrp# match
match/dvmrp/unicast-accept/dvmrppol2# network address 192.31.27.85
mask 255.255.255.0 match exact
network/192.31.27.85/255.255.255.0/exact/dvmrp/unicast-accept/
dvmrppol2#
```

To inject a different network into the DVMRP routing table, navigate to the DVMRP unicast accept policy prompt and enter the following commands:

```
unicast-accept/dvmrppol1/dvmrp# modify
modify/dvmrp/unicast-accept/dvmrppol1# inject address 199.234.64.89
mask 255.255.255.0
inject/199.234.64.89/255.255.255.0/dvmrp/unicast-accept/dvmrppol1#
```

To set a precedence, preference, metric, or type other than the default, follow these examples:

```
unicast-accept/dvmrppol2/dvmrp# precedence 3
unicast-accept/dvmrppol2/dvmrp# preference 8
unicast-accept/dvmrppol2/dvmrp# metric 4
unicast-accept/dvmrpol2/dvmrp# type ospf
```

To ignore a route or interface that matches the DVMRP unicast accept policy dvmrppol2, set the action parameter as follows:

```
box/ip/dvmrp# unicast-accept dvmrppol2
unicast-accept/dvmrppol2/dvmrp# action ignore
```

Using Site Manager

To create or customize a DVMRP unicast accept policy, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Policy Filters.**	The IP Policies menu opens.
4. Choose **DVMRP**.	The DVMRP Policies menu opens.
5. Choose **Unicast Accept Policies**.	The DVMRP Unicast Accept Route Policy Filters window opens.
6. Click on **Add**.	The DVMRP Add Unicast Accept Route Policy Filter window opens.
7. Set the following parameters: • **Name** • **Incoming Networks** • **Action** • **Route Preference** • **Rule Precedence** • **Inject Aggregate** • **Received on Interfaces** • **Route Type** • **Metric** Click on **Help** or see the parameter descriptions beginning on page A-59.	
8. Click on **OK**.	You return to the DVMRP Unicast Accept Route Policy Filters window.
9. Click on **Done**.	You return to the Configuration Manager window.

Disabling or Reenabling DVMRP Unicast Accept Policies

After you create a DVMRP unicast accept policy, you can disable and reenable it.

Using the BCC

To disable a configured unicast accept policy, use state with a value of disabled. For example:

```
box# ip; dvmrp; unicast-accept policy2
unicast-accept/policy2/dvmrp# state disabled
```

To reenable an existing unicast accept policy, use state with a value of enabled.

Using Site Manager

To disable or reenable a DVMRP unicast accept policy, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Policy Filters.**	The IP Policies menu opens.
4. Choose **DVMRP**.	The DVMRP Policies menu opens.
5. Choose **Unicast Accept Policies**.	The DVMRP Unicast Accept Route Policy Filters window opens.
6. Select the name of the DVMRP unicast accept policy that you want to disable or reenable.	Your selection is highlighted.
7. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-59.	
8. Click on **Done**.	You return to the Configuration Manager window.

Configuring DVMRP Accept Policies

A DVMRP accept policy applies to incoming advertisements. To configure a DVMRP accept policy, you can use either the BCC or Site Manager.

Using the BCC

To create a DVMRP accept policy, navigate to the global DVMRP prompt (for example, **box; ip; dvmrp**) and enter:

accept *<polname>*

<polname> is the name of the DVMRP accept policy.

For example, the following command creates a DVMRP accept policy called "dvmrppol3":

```
dvmrp# accept dvmrppol3
accept/dvmrppol3/dvmrp#
```

To customize a DVMRP accept policy, set one or more of the following parameters (Table 4-5):

Table 4-5. DVMRP Accept Policy BCC Parameters

Parameter	Values (default = d)	Description
action	accept (d) | ignore	Specifies whether to accept or ignore the interfaces or networks for a route that matches this policy. • To import the matching route from the IP routing table to the DVMRP routing table, use accept. • If you do not want to import the matching route, use ignore.
gateway	*list of IP addresses* | null (d)	Specifies the addresses of one or more routers that can send DVMRP updates to this router. If you configure a list, this policy applies to DVMRP advertisements from the routers in the list. To apply this policy to any router, use the default, null.
inject	null (d) | *list of IP addresses and masks*	Specifies an IP network that DVMRP injects into the DVMRP routing table in place of the advertised networks. This parameter has meaning only if the action is set to accept. To inject the advertised network, use the default, null. Use this parameter to insert an aggregate or default network along with the actual network.

(continued)

Table 4-5. DVMRP Accept Policy BCC Parameters *(continued)*

Parameter	Values (default = d)	Description
interface	null (d) | *IP address*	To apply the DVMRP accept policy to advertisements that arrive on any interface, use the default, null. Otherwise, use this parameter to specify the IP address of an interface that can receive DVMRP updates to accept or ignore.
metric	1 (d) through 31	Specifies the cost of the route that DVMRP injects into the DVMRP routing table.
network	*address mask* match exact | match range	Specifies the networks that match this policy, and whether you want the match to be exact or a range. • **match exact** means match the specific network advertisement (number and mask). • **match range** means match any network number that falls in the range indicated by the IP address and mask.
precedence	0 (d) through 2,147,483,647	Specifies a metric that DVMRP uses to compare this policy to other policies that match the route. DVMRP uses the precedence value to choose among multiple matches. In ranking policies according to precedence, keep in mind that the route with the highest value is the preferred route. In case of a tie, the route with the larger index number wins.
tunnel	list of tunnels | null (d)	Specifies one or more DVMRP tunnels. If a tunnel interface appears in this list, this policy applies to DVMRP advertisements sent via that tunnel. For each tunnel, enter **local** followed by the local IP address; then enter **remote** followed by the remote IP address. If you want the policy to apply to any tunnel, use the default, null. If you want the policy to apply to no tunnels, enter a tunnel specification consisting of all f's.

Examples

To specify an incoming network address to which this policy applies, navigate to the DVMRP accept policy prompt and enter the following commands:

```
accept/dvmrppol2/dvmrp# match
match/dvmrp/accept/dvmrppol2# network address 192.31.27.85 mask
255.255.255.0 match exact
network/192.31.27.85/255.255.255.0/exact/dvmrp/accept/dvmrppol2#
```

To match any incoming network number that falls within a range, navigate to the DVMRP accept policy prompt and enter the following commands:

```
accept/dvmrppol2/dvmrp# match
match/dvmrp/accept/dvmrppol2# network address 192.31.27.85 mask
255.255.255.0 match range
```

To inject a different network into the DVMRP routing table, navigate to the DVMRP accept policy prompt and enter the following commands:

```
accept/dvmrppol1/dvmrp# modify
modify/dvmrp/accept/dvmrppol1# inject address 199.234.64.89 mask
255.255.255.0
inject/199.234.64.89/255.255.255.0/modify/dvmrp/accept/dvmrppol1#
```

To set a precedence or metric other than the default, follow these examples:

```
accept/dvmrppol2/dvmrp# precedence 3
accept/dvmrppol2/dvmrp# metric 4
```

To ignore the networks, gateways, interfaces, or tunnels that match the DVMRP accept policy dvmrppol2, set the action parameter as follows:

```
box/ip/dvmrp# accept dvmrppol2
accept/dvmrppol2/dvmrp# action ignore
```

Using Site Manager

To create or customize a DVMRP accept policy, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Policy Filters.**	The IP Policies menu opens.
4. Choose **DVMRP**.	The DVMRP Policies menu opens.
5. Choose **Accept Policies**.	The DVMRP Accept Policy Filters window opens.
6. Click on **Add**.	The DVMRP Accept IP Policy Filter Configuration window opens.
7. Set the following parameters: • **Name** • **Action** • **Rule Precedence** • **Incoming Networks** • **Incoming Gateways** • **Received on Interfaces** • **Received on Tunnels** • **Inject Aggregate** • **Metric** Click on **Help** or see the parameter descriptions beginning on page A-64.	
8. Click on **OK**.	You return to the DVMRP Accept Policy Filters window.
9. Click on **Done**.	You return to the Configuration Manager window.

Disabling or Reenabling DVMRP Accept Policies

After you create a DVMRP accept policy, you can disable and reenable it, as needed.

Using the BCC

To disable an existing accept policy, use state with a value of disabled. For example:

```
box# ip; dvmrp; accept policy3
accept/policy3/dvmrp# state disabled
```

To reenable an existing accept policy, use state with a value of enabled.

Using Site Manager

To disable or reenable a DVMRP accept policy, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Policy Filters.**	The IP Policies menu opens.
4. Choose **DVMRP**.	The DVMRP Policies menu opens.
5. Choose **Accept Policies**.	The DVMRP Accept Policy Filters window opens.
6. Select the name of the DVMRP accept policy that you want to disable or reenable.	Your selection is highlighted.
7. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-64.	
8. Click on **Done**.	You return to the Configuration Manager window.

Configuring DVMRP Announce Policies

A DVMRP announce policy governs the propagation of DVMRP routing information. To configure a DVMRP announce policy, you can use either the BCC or Site Manager.

Using the BCC

To create a DVMRP announce policy, navigate to the global DVMRP prompt (for example, **box; ip; dvmrp**) and enter:

announce *<polname>*

<polname> is the name of the DVMRP announce policy.

For example, the following command creates a DVMRP announce policy called "dvmrppol5":

```
dvmrp# announce dvmrppol5
announce/dvmrppol5/dvmrp#
```

To customize a DVMRP announce policy, set one or more of the following parameters (Table 4-6):

Table 4-6. DVMRP Announce Policy BCC Parameters

Parameter	Values (default = d)	Description
action	announce (d) | ignore	Specifies whether to advertise or ignore the interfaces or networks for a route that matches this policy. • To advertise the matching route, use announce. • If you do not want to advertise the matching route, use ignore.
interface	null (d) | *IP address*	Specifies a list of DVMRP interfaces. This policy applies to DVMRP advertisements sent using these interfaces. To apply the DVMRP announce policy to advertisements on any interface, use the default, null.
metric	0 (d) through 31	Specifies a metric for the advertised route. To use the metric values in the routing table, accept the default, 0.

(continued)

Table 4-6. DVMRP Announce Policy BCC Parameters *(continued)*

Parameter	Values (default = d)	Description
network	null (d) | *address mask* match exact | match range	Specifies the networks that match this policy, and whether you want the match to be exact or a range. • **match exact** means match the specific network advertisement (number and mask). • **match range** means match any network number that falls in the range indicated by the IP address and mask. Use the default, null, to match any route.
precedence	0 (d) through 2,147,483,647	Specifies a metric that DVMRP uses to compare this policy to other policies that match the route. DVMRP uses the precedence value to choose among multiple matches. In ranking policies according to precedence, keep in mind that the route with the highest value is the preferred route. In case of a tie, the route with the larger index number wins.
tunnel	*list of tunnels* | null (d)	Specifies one or more DVMRP tunnels. If a tunnel interface appears in this list, this policy applies to DVMRP advertisements sent via that tunnel. For each tunnel, enter **local** followed by the local IP address; then enter **remote** followed by the remote IP address. If you want the policy to apply to any tunnel, use the default, null. If you want the policy to apply to no tunnels, enter a tunnel specification consisting of all f's.

Examples

To specify a network address to which this policy applies, navigate to the DVMRP announce policy prompt and enter the following commands:

```
announce/dvmrppol2/dvmrp# match
match/dvmrp/announce/dvmrppol2# network address 192.31.27.85 mask
255.255.255.0 match exact
network/192.31.27.85/255.255.255.0/exact/dvmrp/announce/dvmrppol2#
```

To match any network number that falls within a range, navigate to the DVMRP announce policy prompt and enter the following commands:

```
announce/dvmrppol2/dvmrp# match
match/dvmrp/announce/dvmrppol2# network address 192.31.27.85 mask
255.255.255.0 match range
```

To advertise a network that is not in the DVMRP routing table, navigate to the DVMRP announce policy prompt and enter the following commands:

```
announce/dvmrppol1/dvmrp# modify
modify/dvmrp/announce/dvmrppol1# advertise address 199.234.64.89 mask
255.255.255.0
advertise/199.234.64.89/255.255.255.0/modify/dvmrp/announce/
dvmrppol1#
```

To set a precedence or metric other than the default, follow these examples:

```
announce/dvmrppol2/dvmrp# precedence 3
announce/dvmrppol2/dvmrp# metric 4
```

To drop advertisements from the tunnels, networks, or interfaces that match the DVMRP announce policy dvmrppol2, set the action parameter as follows:

```
box/ip/dvmrp# announce dvmrppol2
announce/dvmrppol2/dvmrp# action ignore
```

Using Site Manager

To create or customize a DVMRP announce policy, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Policy Filters.**	The IP Policies menu opens.
4. Choose **DVMRP**.	The DVMRP Policies menu opens.
5. Choose **Announce Policies**.	The DVMRP Announce Policy Filters window opens.
6. Click on **Add**.	The DVMRP Announce IP Policy Filter Configuration window opens.
7. Set the following parameters: • **Name** • **Action** • **Rule Precedence** • **Incoming Networks** • **Outgoing Interfaces** • **Outgoing Tunnels** • **Advertise Aggregate** • **Metric** Click on **Help** or see the parameter descriptions beginning on page A-69.	
8. Click on **OK**.	You return to the DVMRP Announce Policy Filters window.
9. Click on **Done**.	You return to the Configuration Manager window.

Disabling or Reenabling DVMRP Announce Policies

After you create a DVMRP announce policy, you can disable and reenable it, as needed.

Using the BCC

To disable an existing DVMRP announce policy, use state with a value of disabled. For example:

```
box# ip; dvmrp; announce policy3
accept/policy3/dvmrp# state disabled
```

To reenable an existing DVMRP announce policy, use state with a value of enabled.

Using Site Manager

To disable or reenable a DVMRP announce policy, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Policy Filters.**	The IP Policies menu opens.
4. Choose **DVMRP**.	The DVMRP Policies menu opens.
5. Choose **Announce Policies**.	The DVMRP Announce Policy Filters window opens.
6. Select the name of the DVMRP announce policy that you want to disable or reenable.	Your selection is highlighted.
7. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-69.	
8. Click on **Done**.	You return to the Configuration Manager window.

Deleting DVMRP

You can use the BCC or Site Manager to delete DVMRP from an IP interface.

Using the BCC

To delete DVMRP from an IP interface, navigate to the DVMRP interface prompt (for example, **box; ethernet/2/2; ip/2.3.4.5/255.255.255.0; dvmrp**) and enter:

delete

For example, the following command deletes DVMRP from IP interface 2.2.2.2/255.255.255.0:

```
dvmrp/2.2.2.2/# delete
ip/2.2.2.2/255.255.255.0#
```

Using Site Manager

To delete DVMRP from an IP interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a connector configured with DVMRP.	The Edit Connector window opens.
2. Choose **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens.
5. Click on **DVMRP**.	Site Manager deselects DVMRP.
6. Click on **OK**.	You return to the Circuit Definition window.
7. Choose **File**.	The File menu opens.
8. Choose **Exit**.	You return to the Configuration Manager window.

Chapter 5
Customizing OSPF Multicast Extensions

MOSPF is a multicasting extension of OSPF. You configure MOSPF by setting OSPF global and interface parameters. This chapter covers the following topics:

Topic	Page
MOSPF Concepts and Terminology	5-2
Configuring MOSPF Globally	5-4
Enabling Multicast Migration Between MOSPF and Nonmulticast Interfaces	5-8
Configuring Multicast Forwarding on an OSPF Interface	5-9
Configuring Multicast-Capable External Routes	5-10
Configuring MOSPF Accept DVMRP Route Policies	5-11

MOSPF Concepts and Terminology

Multicast OSPF (MOSPF) is a multicasting extension of the OSPF protocol that allows a router to forward multicast IP traffic within an OSPF Version 2 autonomous system (AS).

An OSPF environment typically consists of an AS divided into multiple areas connected by an OSPF backbone. You can configure an OSPF/MOSPF router as one of the following:

- Multicasting *internal router* (IR) that establishes neighbor relationships with adjacent routers within an area
- Multicasting *border router* (BR) with interfaces to one or more areas and to the OSPF backbone
- Multicasting *AS boundary router* (ASBR) with one or more interfaces to external autonomous systems

Figure 5-1 shows an OSPF/MOSPF AS consisting of two OSPF areas connected by an OSPF backbone.

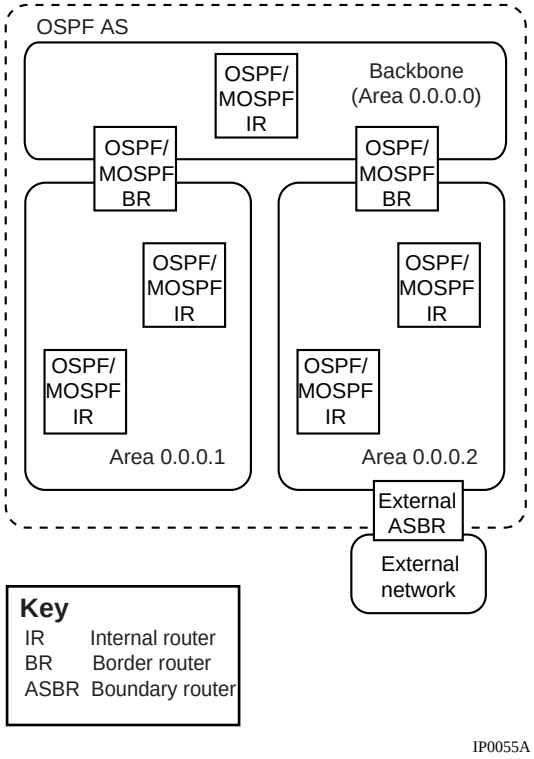

Figure 5-1. OSPF Autonomous System

MOSPF supports four types of multicasting:

- Intra-area multicasting for OSPF internal routers
- Intra-area and inter-area multicasting for OSPF border routers
- Intra-area and inter-AS multicasting for OSPF boundary routers
- All multicasting types

Configuring MOSPF Globally

Bay Networks does not support dynamic configuration of MOSPF. After making local configuration changes, you must restart OSPF by disabling and reenabling it.

If you enable MOSPF, do not run other multicasting protocols on any OSPF interfaces, even if MOSPF is disabled on those interfaces (that is, even if you set the Multicast Forwarding parameter to blocked). If you want to disable MOSPF on a network, use Site Manager to disable MOSPF on all routers in the network.

If you are configuring an OSPF network with both MOSPF and non-MOSPF routers, set the non-MOSPF routers to priority 0 so that the MOSPF routers can become designated router and backup designated router (DR/BDR), which is necessary for MOSPF to work.

To add MOSPF extensions to OSPF, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **OSPF/MOSPF**.	The OSPF menu opens.
4. Choose **Global**.	The Edit OSPF Global Parameters window opens.
5. Set the **Multicast Extensions** parameter. Click on **Help** or see the parameter description on page A-35.	
6. Click on **OK**.	You return to the Configuration Manager window.

After you configure OSPF with multicast extensions, you can set multicast global parameters as described under the following topics:

Topic	Page
Specifying a Forwarding Timeout Value	5-5
Specifying a Maximum Number of Queued Packets	5-6
Enabling Dynamic TTL	5-7

Note: MOSPF will not forward datagrams out an interface until multicast forwarding is enabled on the interface. For instructions, see “Configuring Multicast Forwarding on an OSPF Interface” on page 5-9.

Specifying a Forwarding Timeout Value

To specify a value for timing out MOSPF entries in the forwarding table, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **OSPF/MOSPF**.	The OSPF menu opens.
4. Choose **Global**.	The Edit OSPF Global Parameters window opens.
5. Set the **Multicast Timeout Value** parameter. Click on **Help** or see the parameter description on page A-35.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying a Maximum Number of Queued Packets

By default, MOSPF queues a maximum of 64 packets per slot for all dataflows. You can control how many multicast packets can be queued on each slot for all flows before MOSPF finishes building multicast trees.

- If you disable queuing, packets are dropped before the tree is calculated.
- If you specify a maximum value, the first few data packets for a multicast flow are queued before MOSPF finishes building the multicast tree.

To disable queuing or to specify a different maximum number of queued packets, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **OSPF/MOSPF**.	The OSPF menu opens.
4. Choose **Global**.	The Edit OSPF Global Parameters window opens.
5. Set the **Multicast Max Queued Pkts** parameter. Click on **Help** or see the parameter description on page A-35.	
6. Click on **OK**.	You return to the Configuration Manager window.

Enabling Dynamic TTL

You can configure MOSPF to drop multicast packets that do not have a TTL high enough to reach the closest group member. By default, this feature is disabled.

To enable and disable this feature as required, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **OSPF/MOSPF**.	The OSPF menu opens.
4. Choose **Global**.	The Edit OSPF Global Parameters window opens.
5. Set the **Multicast Dynamic TTL** parameter. Click on **Help** or see the parameter description on page A-36.	
6. Click on **OK**.	You return to the Configuration Manager window.

Enabling Multicast Migration Between MOSPF and Nonmulticast Interfaces

When you globally configure MOSPF, all interfaces running OSPF can receive multicast packets. Remember that IGMP must be configured for all MOSPF interfaces.

Forwarding Multicast Traffic from a Nonmulticast Interface to an MOSPF Interface

To forward multicast packets from a nonmulticast, IGMP static configured interface to an MOSPF configured interface:

- Configure the multicast router as an autonomous system boundary router (ASBR).
- Set the IGMP static forwarding policy for the MOSPF interface with the forwarding mode set to “static to dynamic.”
- Configure the inbound interfaces (using the In Circuits parameter) in the IGMP static forwarding policy.
- Set the IGMP interface parameter Static Forward Cache Lifetime to an appropriate value on the IGMP configured interface (a typical value for MOSPF is 600).
- Enable the Multicast Downstream IGMP Relay parameter in the MOSPF global configuration. This setting allows the source network from which the packet is received to be advertised as multicast-capable, so that the next-hop router in the multicast cloud will not drop the packet because of an unknown source network.

Forwarding Multicast Traffic from an MOSPF Interface to a Nonmulticast Interface

To forward multicast packets from an MOSPF configured interface to a nonmulticast, IGMP static configured interface:

- Set the IGMP static forwarding policy for the MOSPF interface with the forwarding mode set to “dynamic to static.”
- Configure the outbound interfaces in the IGMP static forwarding policy.

Configuring Multicast Forwarding on an OSPF Interface

By default, multicast packets are forwarded on an OSPF interface when you add MOSPF to the router. You can use Site Manager to configure OSPF forwarding on the interface as required.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **OSPF/MOSPF**.	The OSPF menu opens.
4. Choose **Interfaces**.	The OSPF Interfaces window opens.
5. Set the **Multicast Forwarding** parameter. Click on **Help** or see the parameter description on page A-37.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Configuring Multicast-Capable External Routes

By default, all external routes are multicast incapable. The Multicast Downstream IGMP Relay parameter allows you to configure an external route as multicast capable.

If an MOSPF router works as an AS boundary router to support IGMP Relay, you must set this parameter to Enable.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **OSPF/MOSPF**.	The OSPF menu opens.
4. Choose **Global**.	The Edit OSPF Global Parameters window opens.
5. Set the **Multicast Downstream IGMP Relay** parameter. Click on **Help** or see the parameter description on page A-36.	
6. Click on **OK**.	You return to the Configuration Manager window.

Configuring MOSPF Accept DVMRP Route Policies

Use MOSPF accept DVMRP route policies to import DVMRP routes as multicast ASE routes. When connecting an MOSPF domain to an MBone implementation via DVMRP, keep the OSPF database small by configuring an MOSPF accept DVMRP route policy to import only the default DVMRP route to the MOSPF domain.

Creating or Modifying MOSPF Accept DVMRP Route Policies

To create an MOSPF accept DVMRP route policy, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Policy Filters**.	The IP Policies menu opens.
4. Choose **MOSPF**.	The MOSPF Policies menu opens.
5. Choose **Accept DVMRP Route Policies**.	The MOSPF Accept DVMRP Routes Policy Filters window opens.
6. Click on **Add**.	The MOSPF Accept DVMRP Routes Policy Filter Configuration window opens.
7. Set the following parameters: • **Name** • **Action** • **Rule Precedence** • **DVMRP Networks** • **Inject List** Click on **Help** or see the parameter descriptions beginning on page A-73.	
8. Click on **OK**.	You return to the MOSPF Accept DVMRP Routes Policy Filters window.
9. Click on **Done**.	You return to the Configuration Manager window.

Disabling or Reenabling MOSPF Accept DVMRP Route Policies

To disable or reenable an MOSPF accept DVMRP route policy, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Policy Filters.**	The IP Policies menu opens.
4. Choose **MOSPF**.	The MOSPF Policies menu opens.
5. Choose **Accept DVMRP Route Policies**.	The MOSPF Accept DVMRP Routes Policy Filters window opens.
6. Select the name of the MOSPF accept DVMRP route policy that you want to disable or reenable.	Your selection is highlighted.
7. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-73.	
8. Click on **Done**.	You return to the Configuration Manager window.

Chapter 6
Customizing Protocol Independent Multicast

This chapter describes Protocol Independent Multicast-Sparse Mode (PIM-SM) and provides instructions for configuring it.

Topic	Page
PIM Concepts and Terminology	6-2
Customizing PIM Globally	6-19
Customizing PIM on an Interface	6-31
Deleting PIM	6-37

Note: The Bay Networks implementation of PIM supports sparse mode only. In this guide, PIM-SM is referred to as *PIM*.

PIM Concepts and Terminology

PIM, which is defined in RFC 2362, is a multicast routing protocol that efficiently routes packets between members of multicast groups that are sparsely distributed throughout the internetwork. Dense-mode protocols, such as DVMRP, broadcast multicast traffic to all routers over an entire internetwork. PIM sends multicast traffic only to those routers that want to receive traffic for a particular multicast group. PIM reduces the traffic flow over WAN links and reduces overhead costs for processing unwanted multicast packets.

PIM is independent of any specific unicast routing protocol, but does require the presence of a unicast routing protocol somewhere in the internetwork. PIM uses the information from the unicast routing table to create and maintain the shared multicast tree that enables routers to communicate in a PIM network.

The Bay Networks implementation of PIM supports only sparse mode. A typical PIM sparse mode network consists of several multipoint data streams, each targeted to a small number of LANs in the internetwork. For example, customers whose networks consist of multiple hosts on different LANs can use PIM to simultaneously access a video data stream, such as a video teleconference, on a different subnet.

In sparse mode, PIM uses a shared multicast distribution tree that is rooted at the central core point of the PIM network, known as the rendezvous point (RP) router. Sources use RPs routers to identify themselves to other routers on the network; receivers use RPs routers to learn about new sources.

PIM is scalable, making it ideal for a large network, such as an ISP.

This section covers the following topics:

Topic	Page
Components of a PIM Network	6-3
Join/Prune, Register, and Assert Messages	6-7
Shared Trees and Shortest-Path Trees	6-8
How a Receiver Joins a Multicast Group	6-10
How a Receiver Leaves a Multicast Group	6-12
How a Source Sends Multicast Packets to a Group	6-12
How the RP Switches to the Shortest-Path Tree	6-15
How the Last-Hop Router Switches to the Shortest-Path Tree	6-17

Components of a PIM Network

A PIM network consists of the devices described in this section.

Hosts

A host can be either a source or a receiver. A *source* sends multicast data to a multicast group. A source is not required to be a receiver of the group. A source is also known as a *sender.*

A *receiver* wants to receive multicast data from all sources of the multicast group.

Last-Hop Router

The last-hop router is usually the designated router for the receiver side of the network. It is the last router on the path from the source to the receiver.

Designated Router

The *designated router* (DR) is responsible for sending register messages to the RP on behalf of directly connected sources. It is also responsible for sending join/prune messages to the RP on behalf of directly connected receivers. The DR maintains information about the status of the active RP for local sources in each multicast group.

The DR can be a first-hop router, a last-hop router, or both, depending on how you configure your network and which applications you use.

When multiple PIM routers are connected to a multiaccess LAN, PIM elects the router with the highest priority as the DR for the LAN. If two routers have equal priority, then PIM elects the router with the higher IP address as the DR for the LAN.

Rendezvous Point (RP) Routers

Within each domain, PIM builds a shared tree to support a multicast group. At the root of this shared tree is the *rendezvous point* (RP), where receivers meet new sources. When a source wants to announce itself and send data to group members on the shared tree, it sends a register message to the RP. When a receiver wants to receive data for a group, it sends a join message to the RP.

Depending on how you configure your PIM network, an RP can be any PIM router that is physically close to one of the members of the group. An RP can also be another PIM router in the network.

An RP is responsible for specific group prefixes. For example, if you have a network with three RPs, then the group prefixes might be as follows:

- RP1 is responsible for groups 224.0.0.0 through 227.255.255.255.
- RP2 is responsible for groups 228.0.0.0 through 239.255.255.255.
- RP3 is responsible for groups 224.0.0.0 through 239.255.255.255.

You can configure multiple candidate RPs (C-RPs), but only one RP can be active for each multicast group.

For information about configuring a router as an RP, see “Starting PIM” on page 2-7.

Candidate RP Routers

You can configure a set of routers in a PIM domain as candidate RPs (C-RPs). C-RPs periodically send unicast advertisement messages to the bootstrap router (BSR) for that domain. These messages contain the configured Class D group address ranges that the C-RP is responsible for.

You can configure a PIM router to serve as both a C-RP and a C-BSR for one PIM domain. This is the PIM implementation most commonly used.

For information about customizing C-RP configuration parameters, see “Modifying the Candidate RP Configuration” on page 6-26.

Bootstrap Router

The *bootstrap router* (BSR) receives RP advertisement messages from the C-RPs and adds the RP with its group prefix to the RP set. The BSR periodically sends the RP set in bootstrap messages to all routers in the PIM domain. The BSR ensures that all PIM routers learn which RP to send PIM join/prune and register packets to. Only one BSR exists for each PIM domain.

For information about configuring a router as a BSR, see “Starting PIM” on page 2-7.

Candidate Bootstrap Routers

Within a PIM domain, you can configure a small set of routers as candidate BSRs. PIM elects the C-BSR with the highest configured priority as the BSR for the domain. If two C-BSRs have equal priority, then PIM elects the C-BSR with the higher IP address as the BSR for the domain. When you add a new C-BSR with a higher priority to the domain, a new BSR is elected automatically.

For information about customizing BSR configuration parameters, see “Modifying the Candidate BSR Configuration” on page 6-25.

Figure 6-1 shows the devices in a sample PIM network. In this sample network, receivers on LAN A want to simultaneously access the video data stream (video teleconference) connected to LAN B.

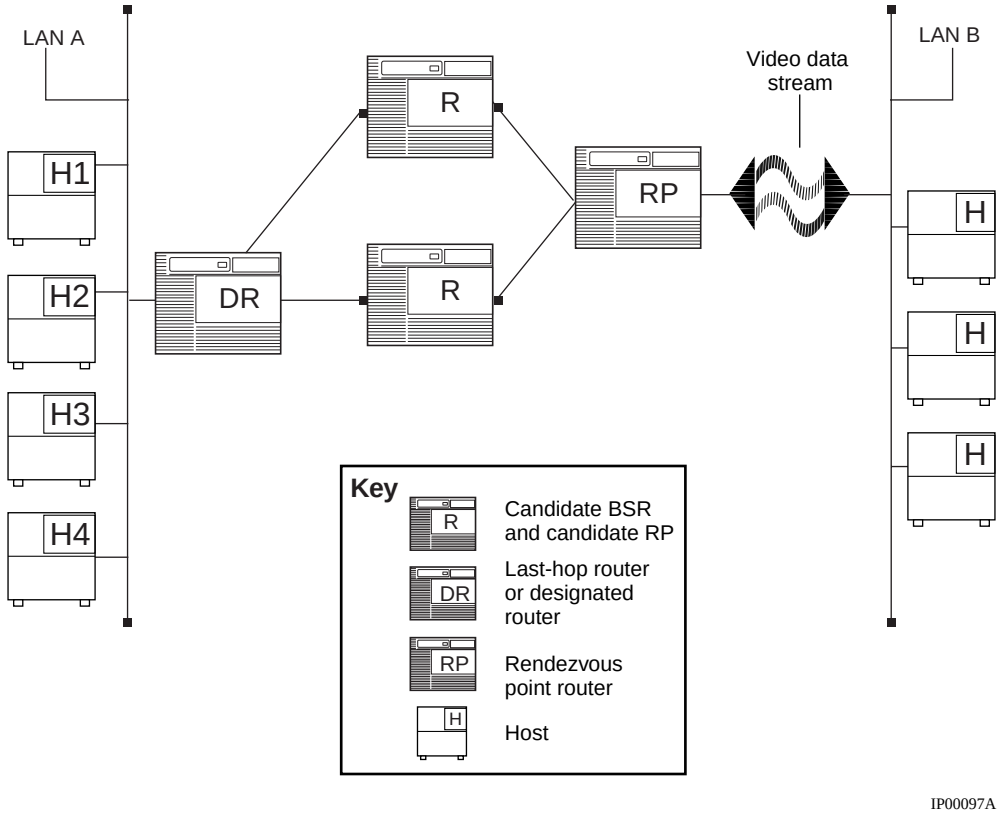

Figure 6-1. PIM Network

Join/Prune, Register, and Assert Messages

PIM routers communicate with each other using the following messages.

Join/Prune Messages

The DR sends *join/prune* messages from a receiver toward a group's RP to either join the shared tree or remove (prune) a branch from it. A single message contains both a join and a prune list. This list includes a set of source addresses, indicating the shortest-path trees (SPTs) or the shared trees that the host wants to join.

The DR sends join and prune messages hop by hop to each PIM router on the path to the source or the RP.

Register and Register-Stop Messages

The DR sends *register* and *register-stop* messages to the RP on behalf of a directly connected source. The register message informs the RP of a new source, causing the RP to send join messages back toward the DR of the source.

The DR stops sending multicast packets after it receives a register-stop message from the RP. The RP sends a register-stop message if there are no downstream receivers for a group, or if the RP has successfully joined the shortest-path tree (SPT).

Assert Messages

PIM uses *assert* messages to determine which of the routers connected to a LAN is responsible for forwarding packets onto the LAN. PIM sends assert messages when two parallel routers have forwarding entries for the same group with outgoing interfaces toward the same LAN.

Shared Trees and Shortest-Path Trees

PIM uses shared trees and shortest-path trees (SPTs) to deliver data packets to group members in a PIM domain. The following sections describe both types of trees.

Shared Trees

By default, group members in a PIM domain receive data from sources across a shared tree. A *shared tree* consists of a set of paths that connect all members of a multicast group to its RP. PIM creates a shared tree when sources and receivers send messages toward the RP. The DR for the source sends register messages, and the DR for the receiver sends join/prune messages. Typically, multicast groups that consist of a large number of low-data-rate sources use shared trees to conserve network resources. A source discovery advertisement application is an example of a low-data-rate source.

Shortest-Path Trees

In general, the shared tree provides an efficient method of forwarding multicast traffic from the source to receivers in a PIM domain. However, when the source begins to send multicast traffic at a high rate, the router can switch from the shared tree to a *shortest-path tree* (SPT) to create a more direct route between itself and the source.

You use SPTs when you want sources and receivers to distribute data at a high rate. Typically, multicast groups that consist of a large number of high-data-rate sources use SPTs. For more information, see “How the RP Switches to the Shortest-Path Tree” on page 6-15 and “How the Last-Hop Router Switches to the Shortest-Path Tree” on page 6-17.

Figure 6-2 shows a shared tree and a shortest-path tree.

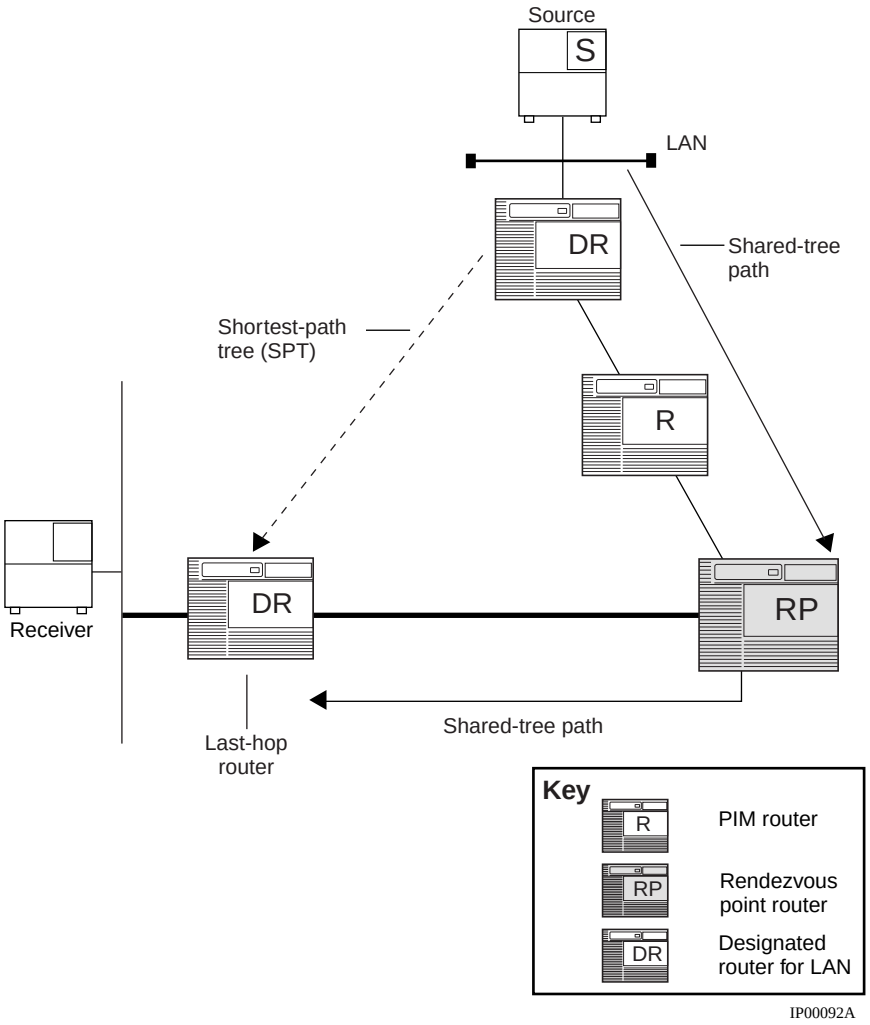

Figure 6-2. Shared Tree and Shortest-Path Tree

How a Receiver Joins a Multicast Group

The following steps, which are illustrated in Figure 6-3, describe how a receiver joins a multicast group:

1. A receiver sends an IGMP host membership message to the DR (normally the last-hop router for that group) on its local interface. The IGMP message contains the address of the multicast group that the receiver wants to join.
2. When the DR receives the IGMP message, it examines the group address and checks the associated group's RP list to determine the RP for the group.
3. After determining the RP for the group, the DR creates a route entry in the multicast forwarding table for the group pair (*, group) and sends a unicast PIM join message directly to the RP. The (*, group) notation indicates any source-group pair.
4. All intermediate routers along the path to the RP create the same entry (*, group) in their multicast forwarding tables. This entry enables the intermediate routers to forward future multicast traffic addressed to the (*, group) pair downstream toward the DR that originated the PIM join message.
5. The RP receives the PIM join message and updates its cache. If the RP knows the requested group, it forwards the multicast packets downstream toward the last-hop router.

Figure 6-3 shows how a receiver joins a group.

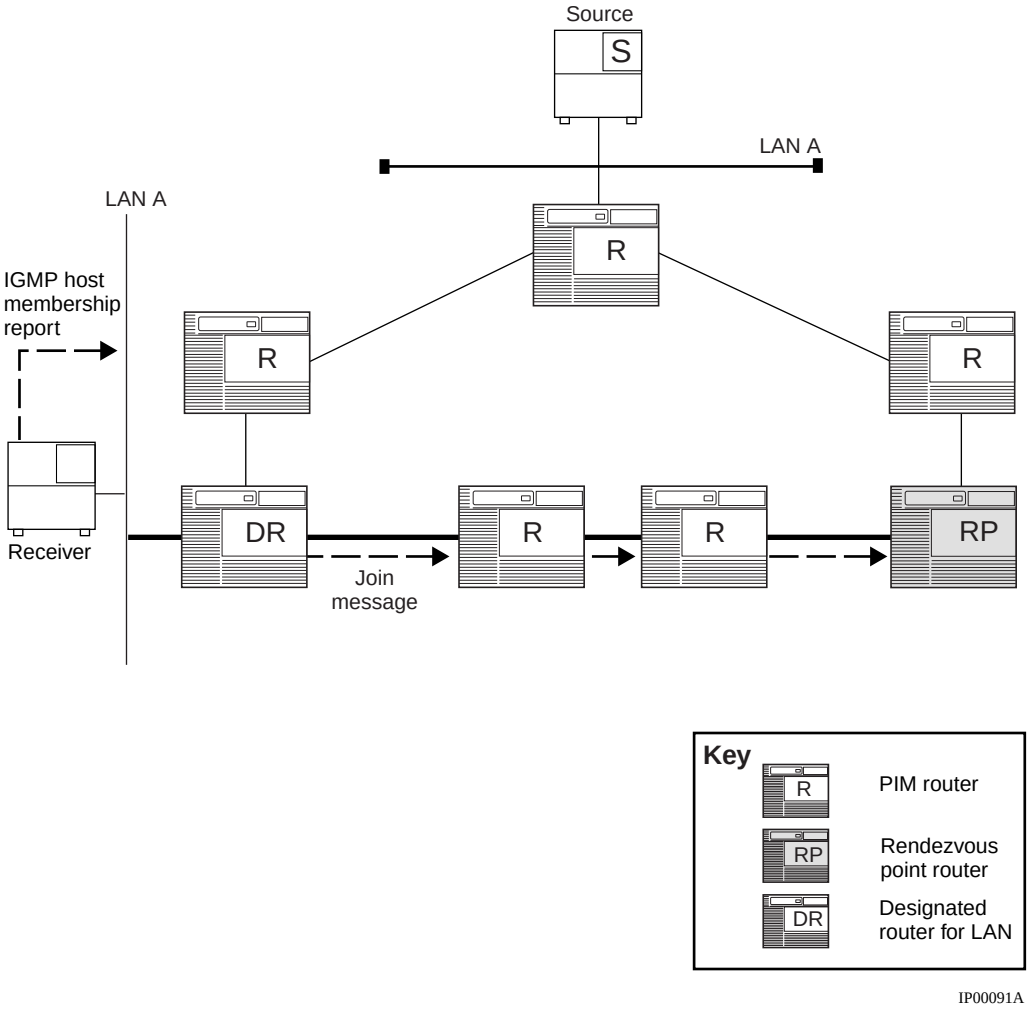

Figure 6-3. How a Receiver Joins a Multicast Group

How a Receiver Leaves a Multicast Group

When a receiver wants to leave a multicast group, it sends an IGMP leave message to the DR.

When all directly connected members of a multicast group leave the group or time out and no downstream members remain, the DR sends a prune message upstream and PIM deletes the route entry after that entry times out.

How a Source Sends Multicast Packets to a Group

The following steps, which are illustrated in Figure 6-4, describe how a source sends multicast packets to a group:

1. A source directly attached to a LAN sends a multicast data packet to the DR. The DR (first-hop router) encapsulates each packet in a register message and sends a unicast message directly to the RP for distribution down the shared tree.
2. The RP responds in the following ways if it has downstream group members that want to receive multicast traffic:
   - If the data rate of the source packet is within the data rate threshold configured on the RP (the default is 1024 bytes per second), the RP decapsulates each register message and forwards native multicast messages downstream to all group members on the shared tree.
   - If the data rate of the source packet exceeds the data rate threshold configured on the RP, the RP can elect to switch to an SPT upon receiving the first packet from the source.

3. If the RP has no downstream members that want to receive multicast traffic for the group, the RP sends a register-stop message to the DR for the source.

   The DR starts the register suppression timer upon receiving the first register-stop message. During the register suppression timeout period (the default is 60 seconds), the following events occur:

   - The source's DR sends a probe packet to the RP before the register suppression timer expires (default is 5 seconds). The probe packet prompts the RP to determine whether any new downstream receivers have joined the group.
   - If no new receivers have joined, the RP sends another register-stop message to the source's DR, and its register suppression timer starts again.
   - When the RP no longer responds to the source DR probe message, the register suppression timer expires and the DR sends encapsulated multicast packets to the RP. The RP uses this method to tell the DR that it has new members that have joined the group.

4. The DR continues to send encapsulated multicast packets to the RP until it receives a register-stop message or a prune message.

Figure 6-4 shows how a source sends multicast packets to a group.

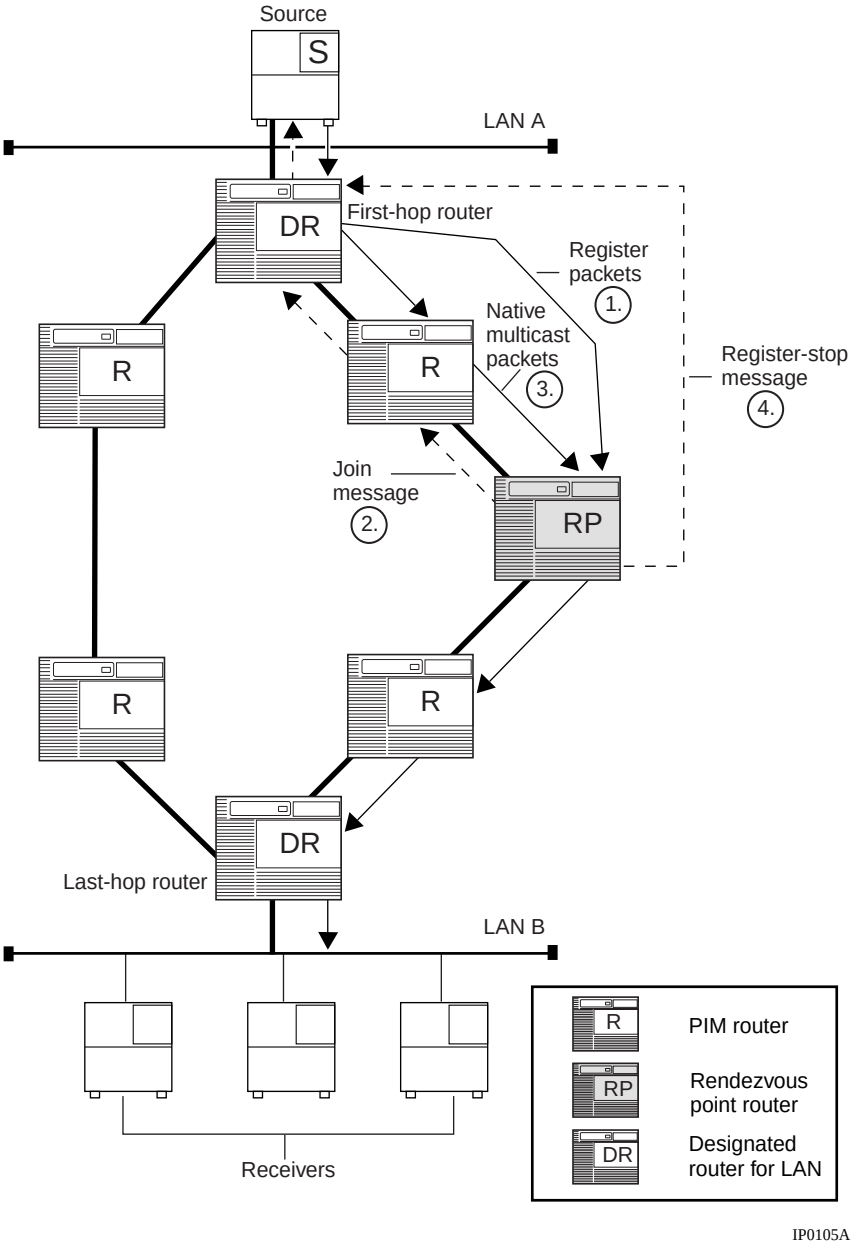

Figure 6-4. How a Source Sends Multicast Packets to a Group

How the RP Switches to the Shortest-Path Tree

The following steps, which are illustrated in Figure 6-5, describe how the RP switches from the shared tree to the shortest-path tree when it has downstream group members:

1. A source directly attached to a LAN sends a multicast packet to a group. The DR (first-hop router) encapsulates each packet in a register message and sends a unicast message directly to the RP for distribution down the shared tree.

   The RP decapsulates each register message and forwards native multicast messages downstream to all members on the shared tree.

2. If the data rate of the source packet exceeds the data rate threshold configured on the RP, the RP immediately sends a join message toward the DR of the source to establish a shortest-path tree between itself and the source.

   All intermediate routers along the path to the source add a new entry to their multicast forwarding tables for the new (source-group) pair. This entry establishes a delivery path that all intermediate routers can use to forward subsequent messages from the source to the RP.

3. After the source's DR receives the join message from the RP, it sends native multicast packets toward the RP on the shortest-path tree.

4. Upon receiving these multicast packets, the RP immediately sends a register-stop message to the DR and then forwards the multicast packets to all downstream group members.

For information about configuring an RP to switch to an SPT, see "Modifying the Rendezvous Point Threshold" on page 6-21.

Figure 6-5 shows how the RP switches to the shortest-path tree.

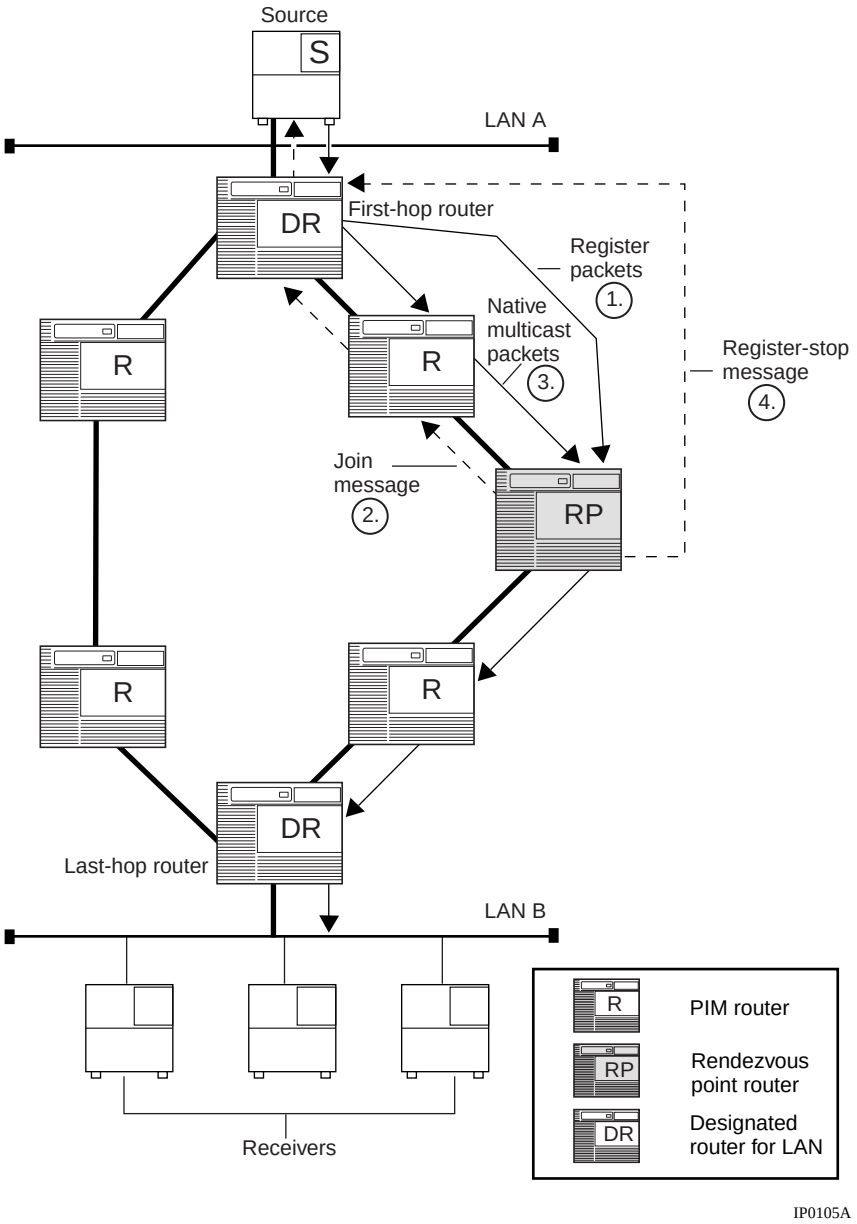

Figure 6-5. How the RP Switches to the Shortest-Path Tree

How the Last-Hop Router Switches to the Shortest-Path Tree

The following steps, which are illustrated in Figure 6-6, describe how the last-hop router switches from the shared tree to the shortest-path tree when it has downstream group members:

1. The last-hop router receives native multicast packets from the RP.
2. If the data rate of the packets sent from the RP exceeds the data threshold configured on the last-hop router, the last-hop router immediately sends a join message toward the DR of the source. This message establishes a shortest-path tree between the source and the last-hop router.

   All intermediate routers along the path to the last-hop router add a new entry (*, group) in their multicast forwarding tables. This entry establishes a delivery path that all intermediate routers can use to forward subsequent messages from the source's DR to the last-hop router on the shortest-path tree.
3. After the source's DR receives the join message from the last-hop router, it sends native multicast packets toward the last-hop router on the shortest-path tree.
4. The last-hop router now receives multicast packets from the RP on the shared tree and from the source's DR on the shortest-path tree. To avoid receiving duplicate packets, the last-hop router sends a prune message toward the RP, indicating that it wants to receive packets on the shortest-path tree only.

For information about configuring a last-hop router to switch to the SPT, see "Modifying the Last-Hop Threshold" on page 6-20.

Figure 6-6 shows how the last-hop router switches to the shortest-path tree.

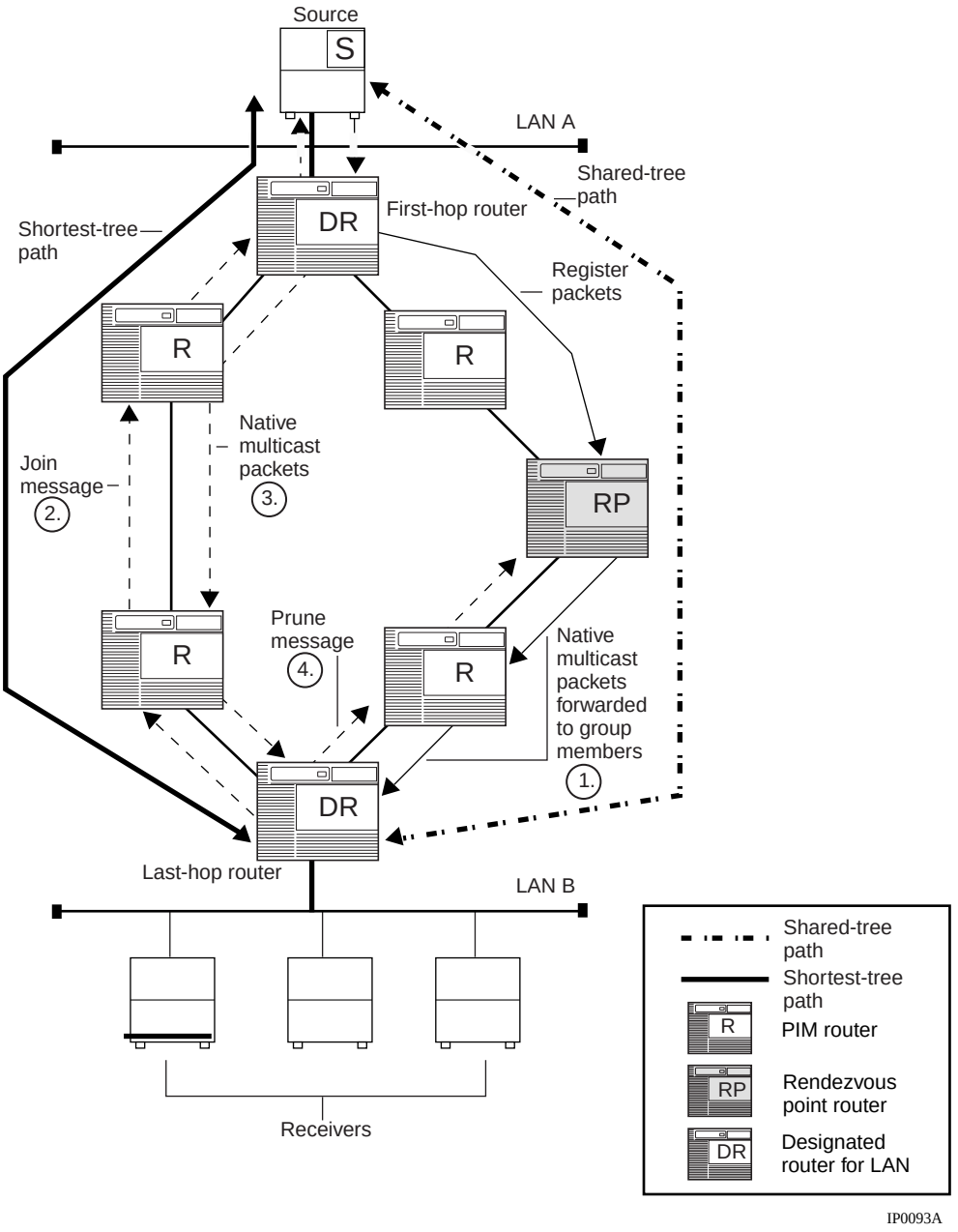

Figure 6-6. How a Last-Hop Router Switches to the Shortest-Path Tree

Customizing PIM Globally

When you enable PIM, default values are in effect for most parameters. You customize PIM by modifying parameters as described under the following topics:

Topic	Page
Disabling and Reenabling PIM Globally	6-20
Modifying the Last-Hop Threshold	6-20
Modifying the Rendezvous Point Threshold	6-21
Specifying the Threshold Sample Interval	6-22
Setting the Default Join/Prune Interval for the Router	6-23
Modifying Neighbor Hello Messages	6-24
Modifying the Candidate BSR Configuration	6-25
Modifying the Candidate RP Configuration	6-26
Setting the Register Suppression Timer	6-27
Setting the Probe Timer	6-28
Enabling and Disabling Cisco Router Compatibility	6-29
Logging PIM Messages	6-30

Disabling and Reenabling PIM Globally

To disable and reenable PIM globally on the router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.
5. Set the **Enable** parameter. Click on Help or see the parameter description on A-37.	
6. Click on **OK**.	You return to the Configuration Manager window.

Modifying the Last-Hop Threshold

By default, a last-hop router switches from the shared tree to a shortest-path tree when the source sends data packets at a rate that exceeds 2048 bytes per second. You can modify the last-hop threshold as follows:

- Change the data threshold rate (bytes per second).
- Specify a value from 0 through 64 for the last-hop data threshold to force the last-hop router to immediately switch from the shared tree to the SPT upon receiving the first packet from the source.
- Disable the last-hop threshold to ensure that PIM routers continue to receive multicast traffic over the shared tree.

For more information about switching from the shared tree to the SPT, see “How the Last-Hop Router Switches to the Shortest-Path Tree” on page 6-17.

To modify the last-hop threshold, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.
5. Set the following parameters: • **Last Hop Threshold** • **Last Hop Data Threshold** Click on **Help** or see the parameter descriptions beginning on page A-38.	
6. Click on **OK**.	You return to the Configuration Manager window.

Modifying the Rendezvous Point Threshold

By default, the RP router switches from the shared tree to the shortest-path tree when the source sends data packets at a rate that exceeds 1024 bytes per second. You can modify the rendezvous point threshold as follows:

- Change the data threshold rate (bytes per second).
- Specify a value from 0 through 64 for the RP data threshold to force the RP to immediately switch from the shared tree to the SPT upon receiving the first packet from the source.
- Disable the RP data threshold to ensure that PIM routers continue to receive multicast traffic over the shared tree.

For more information about switching from the shared tree to the SPT, see “How the RP Switches to the Shortest-Path Tree” on page 6-15.

To modify the RP threshold, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.
5. Set the following parameters: • **Rendezvous Point (RP) Threshold** • **RP Data Threshold** Click on **Help** or see the parameter descriptions beginning on page A-39.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Threshold Sample Interval

The threshold sample interval is the amount of time after which the PIM router calculates the average rate of the current data flow. PIM uses the threshold sample interval to determine the data threshold.

By default, the PIM router calculates the rate of the current data flow at 16-second intervals. You can specify a value from 16 seconds through 300 seconds (5 minutes) to reduce the CPU load from calculation during data forwarding. If you specify a sampling interval that is not a multiple of 16, the PIM router uses the multiple of 16 lower than this value.

To modify the sample threshold interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.
5. Set the **Threshold Sample Interval** parameter. Click on **Help** or see the parameter description on page A-40.	
6. Click on **OK.**	You return to the Configuration Manager window.

Setting the Default Join/Prune Interval for the Router

The join/prune interval is the interval, in seconds, at which each PIM interface configured on a local router sends join/prune messages to its upstream neighbor in the PIM domain.

By default, each PIM interface sends join/prune messages every 60 seconds. You can specify a value from 5 through 18,724 seconds (5 hours, 12 minutes, and 4 seconds).

To modify the join/prune interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Set the **Default Join/Prune Interval** parameter. Click on **Help** or see the parameter description on page A-40.	
6. Click on **OK**.	You return to the Configuration Manager window.

Modifying Neighbor Hello Messages

By default, the Hello messages sent by a PIM router to its neighbors contain a generation identifier. The generation identifier is a random number that PIM appends to Hello messages. This number remains static as long as the router is active. A PIM router uses the generation identifier to quickly learn whether a neighbor rebooted with the latest RP set information within the holdtime specified in its previous Hello message.

You can prevent the PIM router from appending generation identifiers to Hello messages that it sends to its neighbors. Disable this option if you have a network in which Bay Networks and non-Bay Networks PIM routers are interoperating.

To disable and reenable the inclusion of generation identifiers in Hello messages, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.
5. Set the **Generate Neighbor Hello ID** parameter. Click on **Help** or see the parameter description on page A-41.	
6. Click on **OK**.	You return to the Configuration Manager window.

Modifying the Candidate BSR Configuration

A C-BSR is a PIM router that you configure to participate in the BSR election and to serve as the primary BSR, if elected. You can configure multiple routers within a PIM domain as C-BSRs by assigning each an IP address, priority level, interval value, and hash mask length. PIM elects the candidate with the highest priority as the primary BSR for the PIM domain.

To configure a router as a BSR, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.
5. Set the following parameters: • **Candidate BSR** • **Candidate BSR IP Address** • **Candidate BSR Priority** • **Candidate BSR Interval** • **Candidate BSR Hask Mask Length** Click on **Help** or see the parameter descriptions beginning on page A-41.	
6. Click on **OK**.	You return to the Configuration Manager window.

Modifying the Candidate RP Configuration

You can configure a set of PIM routers as C-RPs by assigning each C-RP an IP address, priority level, group mask, advertise interval, and register cache timeout value.

A PIM router can serve as an RP for more than one group, and a group can have more than one RP. Multiple RPs can serve different groups or group ranges or serve as backups to each other.

To configure a router as a candidate RP, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.
5. Set the following parameters: • **Candidate RP** • **Candidate RP IP Address** • **Candidate RP Priority** • **Candidate RP Group/Mask** • **Candidate RP Advertise Interval** • **Candidate RP Register Cache Timeout** Click on **Help** or see the parameter descriptions beginning on A-43.	
6. Click on **OK**.	You return to the Configuration Manager window.

Setting the Register Suppression Timer

The RP sends a register-stop message when it receives native multicast packets from the DR and there are no downstream routers (receivers) to forward these packets to. The source's DR stops the outgoing interface from sending further register packets and sets its register suppression timer. The register suppression timer determines how long the DR waits before sending register messages back to the RP.

The register suppression timer times out when the source's DR no longer receives any register-stop messages during the timeout period. The source's DR then reenables the outgoing interface so that it can send future register packets to the RP.

By default, PIM sets the register suppression timer to 60 seconds. You can set the value from 5 through 65,535 seconds (18 hours, 12 minutes, and 15 seconds).

To set the register suppression timer, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.
5. Set the **Register Suppression Timeout** parameter. Click on **Help** or see the parameter description on page A-46.	
6. Click on **OK**.	You return to the Configuration Manager window.

Setting the Probe Timer

The probe timer specifies the interval, in seconds, between the time that the first-hop router sends a probe packet to the RP router and the expiration of the register suppression timer.

Before the register suppression timer times out, the first-hop router sends a probe packet to the RP. If the RP determines that it still does not have any downstream receivers, it sends a register-stop message back to the first-hop router, thereby restarting the suppression timer. If the first-hop router does not receive a register-stop message in response to the probe, the suppression timer expires and the first-hop router re-creates the outgoing interface for this entry so that future register packets can be forwarded to the RP router.

By default, PIM sets the probe timer to 5 seconds. You can set the probe timer from 1 through 65,535 seconds (18 hours, 12 minutes, and 15 seconds). This value must be less than the value you specify for the register suppression timer. Otherwise, the probe timer has no effect and the register suppression timer times out.

To set the probe timer, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.
5. Set the **Probe Time** parameter. Click on **Help** or see the parameter description on page A-47.	
6. Click on **OK**.	You return to the Configuration Manager window.

Enabling and Disabling Cisco Router Compatibility

By default, Bay Networks routers are compatible with the standard PIM specification defined in RFC 2362. You can enable Bay Networks routers to interoperate with Cisco routers configured with a nonstandard PIM implementation.

To enable or disable Cisco router compatibility, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.
5. Set the **Cisco Compatible** parameter. Click on **Help** or see the parameter description on page A-47.	
6. Click on **OK**.	You return to the Configuration Manager window.

Logging PIM Messages

By default, PIM does not log PIM informational/warning, debug, or trace messages.

To enable the logging of PIM informational/warning, debug, and trace messages, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.
5. Set the following parameters: • **Info/Warnings** • **Debug** • **Trace** Click on **Help** or see the parameter descriptions beginning on page A-48.	
6. Click on **OK**.	You return to the Configuration Manager window.

Customizing PIM on an Interface

You customize PIM on an interface by modifying PIM parameters as described under the following topics:

Topic	Page
Disabling and Reenabling PIM on an Interface	6-31
Setting the Hello Interval	6-32
Setting the Cache Timeout Interval	6-33
Setting the Join/Prune Interval for an Interface	6-34
Enabling and Disabling IGMP Relay on a Downstream Router	6-35
Specifying the Local DR Priority	6-36

Disabling and Reenabling PIM on an Interface

By default, PIM is enabled on an interface. To disable and reenable PIM on an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Interface**.	The PIM Interface Parameters window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-51.	
6. Click on **OK**.	You return to the Configuration Manager window.

Setting the Hello Interval

The Hello interval specifies how often the local router sends PIM Hello messages on this PIM interface to neighboring routers in the PIM domain. PIM routers periodically send Hello messages so that PIM neighbors can discover each other. Hello messages are multicast using address 224.0.0.13 (all PIM routers group) and are sent on all communication links.

By default, the local router sends Hello messages on this PIM interface every 30 seconds. You can set the value from 1 through 2,147,483,647 seconds. Bay Networks recommends a higher value for slower-speed serial lines.

To specify the Hello interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Interface**.	The PIM Interface Parameters window opens.
5. Set the **Hello Interval** parameter. Click on **Help** or see the parameter description on page A-51.	
6. Click on **OK**.	You return to the Configuration Manager window.

Setting the Cache Timeout Interval

The cache timeout interval determines how long PIM data entries remain in the PIM cache before they time out. By default, entries remain in the cache for 210 seconds. You can specify a value from 5 through 2,147,483,647 seconds.

To set the cache timeout interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Interface**.	The PIM Interface Parameters window opens.
5. Set the **Cache Time Out** parameter. Click on **Help** or see the parameter description on page A-52.	
6. Click on **OK**.	You return to the Configuration Manager window.

Setting the Join/Prune Interval for an Interface

The join/prune interval is the interval, in seconds, at which each PIM interface on the router sends periodic join/prune messages to its upstream neighbor. By default, PIM interfaces use the join/prune interval configured for the entire router (see "Setting the Default Join/Prune Interval for the Router" on page 6-23).

You can set a different join/prune interval on a PIM interface by disabling the use of the global interval on that interface and specifying another interval. You can specify an interval from 1 through 65,535 seconds (18 hours, 12 minutes, and 15 seconds); the default interval is 60 seconds.

To specify a join/prune interval for an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Interface**.	The PIM Interface Parameters window opens.
5. Set the **Use Global Join/Prune Interval** parameter to **Disable**. Click on **Help** or see the parameter description on page A-52.	
6. Set the **Join/Prune Interval** parameter. Click on **Help** or see the parameter description on page A-53.	
7. Click on **OK**.	You return to the Configuration Manager window.

Enabling and Disabling IGMP Relay on a Downstream Router

An IGMP Relay device is a unicast router with an interface to a multicast router and interfaces to one or more networks containing network hosts. A router configured as an IGMP Relay device provides group registration services for an IP multicast router in a PIM environment. For more information about IGMP Relay, see Chapter 9, “Configuring IGMP Relay.”

By default, IGMP Relay support for downstream routers is disabled. When you enable IGMP Relay support for a downstream router, PIM receives multicast data from the downstream router, encapsulates the data within a register packet, and sends the packets to the elected RP in the PIM domain.

To enable and disable IGMP Relay support for a downstream router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Interface**.	The PIM Interface Parameters window opens.
5. Set the **Downstream IGMP Relay** parameter. Click on **Help** or see the parameter description on page A-53.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Local DR Priority

The local DR priority indicates the priority level for a DR on the LAN. The higher the number, the higher the priority.

A PIM router configured with a DR election priority sends to its PIM neighbors a Hello message that contains its priority level. The PIM router with the highest priority level is elected the DR for the LAN. Local routers not configured with a DR election priority level elect a DR based on the highest IP address.

By default, the local DR priority is 1. You can specify a priority value from 1 through 65,535 for a PIM router. To disable the DR election priority level on the LAN, enter a priority value of 0.

To set the DR election priority level, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Interface**.	The PIM Interface Parameters window opens.
5. Set the **Local DR Priority** parameter. Click on **Help** or see the parameter description on page A-54.	
6. Click on **OK**.	You return to the Configuration Manager window.

Deleting PIM

To delete PIM from an IP interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a connector configured with PIM.	The Edit Connector window opens.
2. Choose **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens.
5. Click on **PIM**.	Site Manager deselects PIM.
6. Click on **OK**.	You return to the Circuit Definition window.
7. Choose **File**.	The File menu opens.
8. Choose **Exit**.	You return to the Configuration Manager window.

Chapter 7
Configuring RSVP

The Resource Reservation Protocol (RSVP) allows host systems in an IP network to reserve resources on RSVP-capable routers for:

- Unicast dataflows
- Multicast dataflows

A dataflow is a transmission of packets from a source to one or more destinations requiring a specific quality of service (QoS).

This chapter covers the following topics:

Topic	Page
How RSVP Works	7-2
Configuring RSVP Globally	7-4
Configuring RSVP on an Interface	7-7
Deleting RSVP	7-14

How RSVP Works

A network host that wants to establish a dataflow with a specified QoS sends an RSVP path message addressed to a potential receiving host or group of hosts. In Figure 7-1, for example, a host sends a multicast RSVP path message to a group of four hosts. Routers in the network receive the multicast RSVP messages and forward them to the next-hop router until the messages reach their host destinations. The sequence of networks and routers that a path message traverses from source to destination establishes the path for the proposed dataflow.

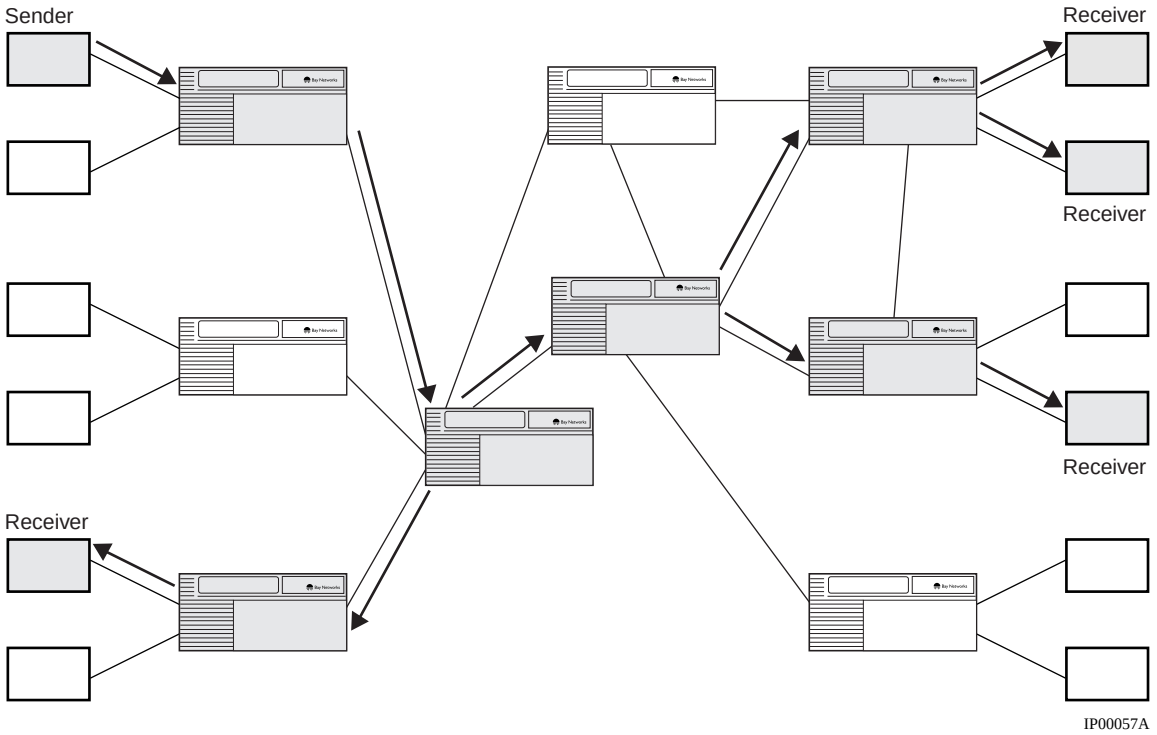

Figure 7-1. RSVP Path Message

A network host that receives an RSVP path message decides whether it wants to receive data on the proposed dataflow. If so, the host returns an RSVP reserve message. In Figure 7-2, for example, each host that received an RSVP path message returns a reserve message. Each router in the network:

1. Passes the reservation request to the local Circuit Resource Manager (CRM)
2. Forwards the reservation request to the previous hop in the flow (as determined by the earlier path message)

In this manner, the reserve message traces the data path set up by the corresponding path message and establishes resource reservation along the data path at each router. Note that reservations from multiple receivers may be merged on their way to the sender of the path message.

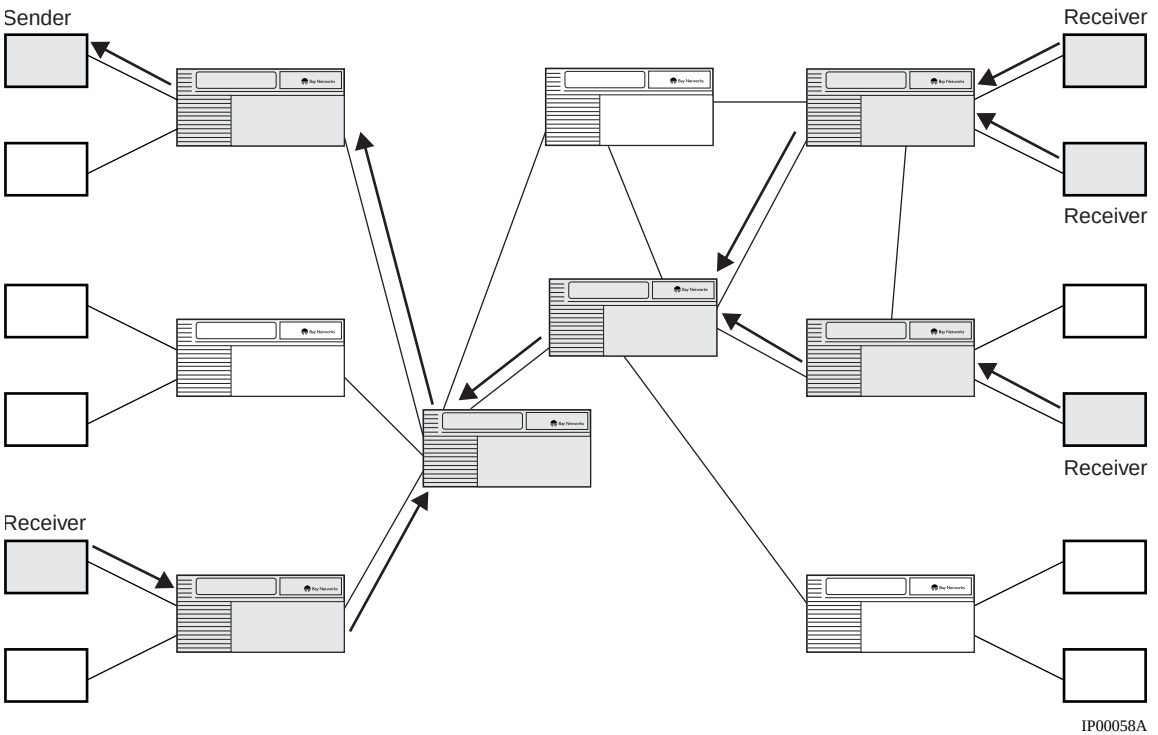

Figure 7-2. RSVP Reserve Message

Configuring RSVP Globally

When you start RSVP on the router, RSVP runs with default values for all global parameters. You customize RSVP by modifying parameters as described under the following topics:

Topic	Page
Disabling and Reenabling RSVP	7-4
Choosing a Slot	7-5
Logging RSVP Messages	7-6

Disabling and Reenabling RSVP

By default, RSVP is enabled on the router.

To disable or reenable RSVP, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **RSVP**.	The RSVP menu opens.
4. Choose **Global**.	The RSVP Base Group Record window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-54.	
6. Click on **Save**.	You return to the Configuration Manager window.

Choosing a Slot

By default, RSVP runs on every slot where it is configured.

To specify the slot or slots on which you want RSVP to run, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **RSVP**.	The RSVP menu opens.
4. Choose **Global**.	The RSVP Base Group Record window opens.
5. Set the **Soloist Slots** parameter. Click on **Help** or see the parameter description on page A-55.	
6. Click on **Save**.	You return to the Configuration Manager window.

Logging RSVP Messages

By default, the router does not log RSVP messages (informational, debug, and trace). To enable the logging of informational, debug, and trace messages for RSVP components, complete the following tasks:

Caution: Enabling message logging increases the chance of losing information because of lack of memory.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **RSVP**.	The RSVP menu opens.
4. Choose **Global**.	The RSVP Base Group Record window opens.
5. Set the following parameters: • **Info Log Filter** • **Debug Log Filter** • **Trace Log Filter** Click on **Help** or see the parameter descriptions beginning on page A-55.	
6. Click on **Save**.	You return to the Configuration Manager window.

Configuring RSVP on an Interface

When you add RSVP to an IP interface, RSVP is configured with default values for all interface parameters. You customize RSVP on the interface by setting interface parameters as described under the following topics:

Topic	Page
Disabling and Reenabling RSVP on an Interface	7-7
Setting the RSVP Default Refresh Timer	7-8
Setting the RSVP Default Lifetime Multiplier	7-9
Setting the RSVP Refresh Blockade Multiplier	7-10
Setting the TTL Override	7-11
Setting the Route Delay Value	7-12
Enabling and Disabling UDP Encapsulation	7-13

Disabling and Reenabling RSVP on an Interface

By default, RSVP is enabled on every interface on which it is configured. To disable or reenable RSVP on an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **RSVP**.	The RSVP menu opens.
4. Choose **Circuit**.	The Edit RSVP Circuit Parameters window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-56.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Setting the RSVP Default Refresh Timer

RSVP sends periodic refresh messages to maintain the state along a reserved path. Without periodic refreshment, the state automatically times out.

The refresh timer interval is expressed in hundredths of a second. By default, the RSVP refresh timer is set to 3000 hundredths of a second (30 seconds).

To set the refresh timer for an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **RSVP**.	The RSVP menu opens.
4. Choose **Circuit**.	The Edit RSVP Circuit Parameters window opens.
5. Set the **Refresh Interval** parameter. Click on **Help** or see the parameter description on page A-57.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Setting the RSVP Default Lifetime Multiplier

The lifetime multiplier is an integer that multiplies the TIME_VALUE object specified in a path or reserve message. The resulting value indicates the amount of time that the router will hold the path or reserve state without receiving a refresh message for that state.

By default, the lifetime multiplier is 3. To specify a different multiplier, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **RSVP**.	The RSVP menu opens.
4. Choose **Circuit**.	The Edit RSVP Circuit Parameters window opens.
5. Set the **Refresh Multiple** parameter. Click on **Help** or see the parameter description on page A-57.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Setting the RSVP Refresh Blockade Multiplier

By default, an RSVP interface in the blockade state stays alive for four refresh intervals.

To change the refresh blockade multiplier, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **RSVP**.	The RSVP menu opens.
4. Choose **Circuit**.	The Edit RSVP Circuit Parameters window opens.
5. Set the **Refresh Blockade Multiple** parameter. Click on **Help** or see the parameter description on page A-56.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Setting the TTL Override

By default, RSVP uses the IP TTL value. To override this value, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **RSVP**.	The RSVP menu opens.
4. Choose **Circuit**.	The Edit RSVP Circuit Parameters window opens.
5. Set the **RSVP TTL** parameter. Click on **Help** or see the parameter description on page A-57.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Setting the Route Delay Value

The route delay value specifies the approximate period that elapses between the time that a route is changed and the time that a resulting message appears on the interface.

The route delay is expressed in hundredths of a second. By default, the route delay is 200 hundredths of a second (2 seconds). To specify a different delay, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **RSVP**.	The RSVP menu opens.
4. Choose **Circuit**.	The Edit RSVP Circuit Parameters window opens.
5. Set the **Route Delay** parameter. Click on **Help** or see the parameter description on page A-58.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Enabling and Disabling UDP Encapsulation

By default, RSVP uses UDP encapsulation on this interface only if it determines that a neighbor on the interface uses UDP encapsulation. Enable this feature on the interface if manual configuration requires UDP encapsulation.

To enable and disable UDP encapsulation on the interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **RSVP**.	The RSVP menu opens.
4. Choose **Circuit**.	The Edit RSVP Circuit Parameters window opens.
5. Set the **Udp Required** parameter. Click on **Help** or see the parameter description on page A-58.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Deleting RSVP

To delete RSVP from an IP interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a connector configured with RSVP.	The Edit Connector window opens.
2. Choose **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens.
5. Click on **RSVP**.	Site Manager deselects RSVP.
6. Click on **OK**.	You return to the Circuit Definition window.
7. Choose **File**.	The File menu opens.
8. Choose **Exit**.	You return to the Configuration Manager window.

Chapter 8
Reserving Line Resources

This chapter covers the following topics:

Topic	Page
About Line Resource Reservation	8-2
How the Resource Manager Works with RSVP	8-3
Setting the Estimated Bandwidth	8-4
Setting the Reservable Bandwidth	8-5
Specifying the Traffic Queuing Algorithm	8-6
Specifying the LRM Policing Algorithm	8-7
Setting the Bandwidth Interval	8-8
Setting the Inflate Reservations Percentage	8-9
Specifying the Unreserved Policing Algorithm	8-10
Specifying the Unreserved Queue Length	8-11
Specifying the Multiline Select Algorithm	8-12
Setting the Multiline Threshold Bandwidth	8-13
Setting the Reservation Latency	8-14
Setting the Maximum Reservable Bandwidth for a Dataflow	8-15
Setting the Maximum Buffer Space for a Dataflow	8-16

About Line Resource Reservation

Emerging real-time multicast applications for digitized voice and video (such as multimedia conferencing and virtual reality) require a level of consistent network service that routers cannot meet using simple first-in-first-out (FIFO) queuing mechanisms. The existing best-effort delivery service of IP networks, where variable queuing delays and data loss due to congestion are acceptable, is not sufficient.

Resource reservation protocols such as RSVP address the requirements of delay-sensitive applications by distributing information among routers to achieve a guaranteed quality of service (QoS) for specific packet streams (flows).

By reserving bandwidth for QoS requests, a system of line resource reservation can meet the demands of real-time applications and maintain bandwidth for other traffic.

Bay Networks line resource reservation supports bandwidth guarantees only. It does not support delay guarantees.

Resource Manager

The Bay Networks Resource Manager lets you define a certain percentage of a line's bandwidth as *reservable*. Applications that require a guaranteed QoS can negotiate for the reservable bandwidth. When the router honors a reservation request, the Resource Manager allocates bandwidth from the reservable bandwidth, reducing the bandwidth available for other requests.

Supported Media

You must enable the Resource Manager on 10 Mb/s and 100 Mb/s Ethernet, FDDI, MCT1, HSSI, and synchronous interfaces that are configured with RSVP. The Resource Manager supports the following synchronous interface encapsulation methods:

- Point-to-Point Protocol (PPP)
- Bay Networks Standard
- FDDI
- 100 Mb/s Ethernet

Note: You cannot use line resource management on a line configured for PPP multilink.

How the Resource Manager Works with RSVP

The exchange between RSVP and the Resource Manager consists of the following steps:

1. The router receives an RSVP reserve message. The reserve message includes a flow specification (*flowspec*) that indicates the resources needed to meet the QoS.
2. RSVP passes the flowspec to the Resource Manager.
3. The Resource Manager compares the requested resources with available reservable bandwidth. The Resource Manager determines reservable bandwidth from configured values described later in this chapter. It also accounts for any active reserved flows.
4. The Resource Manager either reserves the necessary services or refuses service.

Setting the Estimated Bandwidth

To activate resource reservation, select a line and enter the portion of the line's bandwidth to make available for RSVP requests.

Enter an estimated total bandwidth for this line, from 0 through 214,748,364 bits per second. To enable line resource management, enter a value greater than 0.

- For point-to-point lines, you can usually enter the total line speed.
- For an Ethernet line, you must estimate a value, because shared-media lines may not have all of the bandwidth available. Base the estimate on line statistics, the number of connected workstations, or other site-specific information.

To set the estimated bandwidth, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Estimated Bandwidth** parameter. Click on **Help** or see the parameter description on page A-28.	
4. Click on **OK**.	You return to the Configuration Manager window.

Setting the Reservable Bandwidth

To enable RSVP reservable resources, specify the portion of this line's bandwidth to make available for RSVP requests for guaranteed service. The value can be any integer from 0 through 214,748,364 bits per second and must be less than the value of the Estimated Bandwidth parameter.

Caution: Never make all available bandwidth reservable. Leave at least 15 percent of bandwidth available for network management, routing protocols, and other best-effort traffic.

To set the reservable bandwidth, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Reservable Bandwidth** parameter. Click on **Help** or see the parameter description on page A-29.	
4. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Traffic Queuing Algorithm

By default, the Line Resource Manager (LRM) schedules reserved traffic ahead of unreserved traffic. You can configure the LRM to use best-effort scheduling for all reserved traffic.

To specify the traffic queuing algorithm, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Traffic Queuing Algorithm** parameter. Click on **Help** or see the parameter description on page A-29.	
4. Click on **OK**.	You return to the Configuration Manager window.

Specifying the LRM Policing Algorithm

By default, LRM uses the leaky bucket policing algorithm for reserved traffic to make sure that all traffic using reserved bandwidth follows the flowspec that appears in the reserve message. For the controlled load service, LRM attempts to carry any packets that do not adhere to the flowspec.

You can disable the policing algorithm if you know that an upstream router is policing traffic, or that the applications generating the reserved traffic consistently adhere to the flowspec and do not require policing.

Note that leaky bucket policing requires additional processing by the router.

To specify the LRM policing algorithm, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Policing Algorithm** parameter. Click on **Help** or see the parameter description on page A-30.	
4. Click on **OK**.	You return to the Configuration Manager window.

Setting the Bandwidth Interval

By default, LRM measures instantaneous bandwidth over a 10-second interval. If 10 seconds is not sufficient, you can specify a different bandwidth interval for this interface, from 1 through 214,748,364 seconds (nearly 7 years).

To set the bandwidth interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Bandwidth Interval (Secs**) parameter. Click on **Help** or see the parameter description on page A-30.	
4. Click on **OK**.	You return to the Configuration Manager window.

Setting the Inflate Reservations Percentage

By default, LRM does not add a safety tolerance to each RSVP reservation on a line. To inflate (or overallocate) reservations made on this line, enter a percent value to increase each bandwidth request.

Increase the value of this parameter if you notice that LRM is discarding packets because applications generating reserved traffic are exceeding their flowspecs.

To set the inflate reservations percentage, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Inflate Reservations Percentage** parameter. Click on **Help** or see the parameter description on page A-31.	
4. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Unreserved Policing Algorithm

LRM uses one of two policing algorithms for unreserved traffic:

- *Queue limit* -- Restricts the number of buffers (packets) of unreserved traffic that LRM queues

  This method of policing enables unreserved traffic to use available reserved bandwidth.

Note: If you enable priority queuing for this line, the router uses the priority queue parameters to perform queue limit policing. See *Configuring Traffic Filters and Protocol Prioritization* for information about priority queue parameters.

- *Leaky bucket* -- Causes the router to actively police the unreserved traffic based on the unreserved bandwidth

  This method does not allow unreserved traffic to take advantage of available reserved bandwidth.

To specify the unreserved policing algorithm, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Unreserved Policing Algorithm** parameter. Click on **Help** or see the parameter description on page A-31.	
4. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Unreserved Queue Length

If the Unreserved Policing Algorithm parameter is set to Queue Limit, you can specify the maximum number of unreserved (best-effort) packets to be held in queue for transmission. After the queue length reaches this value, the router discards best-effort traffic when congestion occurs.

Note that priority queuing limits, if configured, override the value of this parameter.

By default, LRM holds a maximum of 20 unreserved packets in queue for transmission. Change this value to adjust the queue length limit from 0 through 214,748,364 packets (limited by available buffers).

To specify the unreserved queue length, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Unreserved Queue Length** parameter. Click on **Help** or see the parameter description on page A-32.	
4. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Multiline Select Algorithm

If you configured LRM on a multiline circuit, you can choose one of two algorithms that determine how LRM selects which line to use for a new resource request:

- *First fit* -- Always uses the first available line that can service reserved traffic requests
- *Round robin* -- Rotates the use of lines available to service requests

All lines for a circuit must use the same algorithm. If any one line on a circuit specifies First Fit, all lines use the first fit algorithm.

To specify the multiline select algorithm, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Multiline Select Algorithm*** parameter. Click on **Help** or see the parameter description on page A-32.	
4. Click on **OK**.	You return to the Configuration Manager window.

* You set this parameter only if you configured the Resource Manager on a multiline circuit.

Setting the Multiline Threshold Bandwidth

When using the first fit multiline select algorithm (see “Specifying the Multiline Select Algorithm” on page 8-12), you can configure a threshold from 0 through 214,748,364 bits per second for the first available line.

By default, the threshold is set to 0; LRM uses the simple first fit algorithm. If you select a value greater than 0, LRM still uses the first available line with reservable bandwidth to service requests, but moves to the next available line after reaching the configured threshold. When all lines are at their threshold, LRM returns to using the simple first fit algorithm.

Set this parameter only if you configured LRM on a multiline circuit and set the Multiline Select Algorithm parameter to First Fit.

To set the multiline threshold bandwidth, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Multiline Threshold Bandwidth*** parameter. Click on **Help** or see the parameter description on page A-33.	
4. Click on **OK**.	You return to the Configuration Manager window.

* You set this parameter only if you configured the Resource Manager on a multiline circuit.

Setting the Reservation Latency

By default, the maximum latency for a reserved flow packet is 50 milliseconds (ms), limiting the amount of unreserved data that the link scheduler can transmit. When the data transmit ring reaches a size where the time to transmit the data is greater than the value of this parameter, no more unreserved data will be queued.

You can set the reservation latency from 0 through 214,748,364 ms. Reduce the value of this parameter to obtain better delay characteristics for reserved flows, but note that overall throughput may decrease. Increase the default value to improve throughput, but note that reserved-flow delays may increase.

To set the reservation latency, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Reservation Latency** parameter. Click on **Help** or see the parameter description on page A-33.	
4. Click on **OK**.	You return to the Configuration Manager window.

Setting the Maximum Reservable Bandwidth for a Dataflow

By default, there is no maximum amount of bandwidth that can be reserved by a flow.

To specify the maximum reservable bandwidth, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Largest Bandwidth** parameter. Click on **Help** or see the parameter description on page A-34.	
4. Click on **OK**.	You return to the Configuration Manager window.

Setting the Maximum Buffer Space for a Dataflow

By default, there is no maximum amount of buffer space that can be used by a flow.

To specify the maximum buffer space for a flow, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on any connector for a line that is configured for RSVP.	The Edit Connector window opens.
2. Click on **Edit Line Resources** in the Edit Connector window.	The Edit Line Resources window opens.
3. Set the **Largest Buffer** parameter. Click on **Help** or see the parameter description on page A-34.	
4. Click on **OK**.	You return to the Configuration Manager window.

Chapter 9
Configuring IGMP Relay

This chapter consists of the following topics:

Topic	Page
IGMP Relay Overview	9-2
Enabling and Disabling IGMP Relay Globally	9-9
Specifying a Timeout Value for Multicast Table Entries	9-11
Configuring Upstream Data Forwarding	9-12
Specifying the Relay Interface Type	9-13
Configuring Unsolicited Reports on an Upstream Interface	9-16
Configuring MOSPF for Use with IGMP Relay	9-18
Configuring a DVMRP Router for Use with IGMP Relay	9-20
Configuring a Backup Multicast Router	9-22
Configuring IGMP Relay with Router Redundancy	9-23

IGMP Relay Overview

An IGMP Relay device is a unicast router with an interface to a multicast router and interfaces to one or more networks containing network hosts. Figure 9-1 shows an IGMP Relay device connected to three LANs containing host systems.

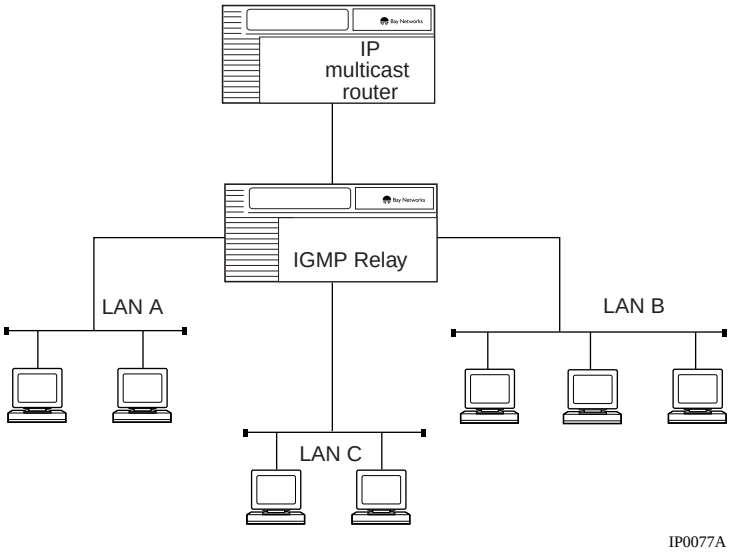

Figure 9-1. IGMP Relay Device

The IGMP Relay device provides the following group registration services for an IP multicast router:

- Sends IGMP host membership queries to hosts on its attached local networks
- Receives host membership reports and unsolicited join messages from hosts on its attached networks and forwards them to the attached multicast router
- Forwards multicast data to group members on locally attached networks

For more information about IGMP, see Chapter 3, “Configuring and Customizing IGMP.”

IGMP Relay concepts, terminology, functions, and components are discussed under the following topics:

Topic	Page
IGMP Relay Topology	9-3
How IGMP Relay Works	9-4
Unicast Routing Protocols on the IGMP Relay Device	9-8
Routing Protocols on the Multicast Router	9-8

IGMP Relay Topology

An IGMP Relay device is located physically between the IGMP hosts and the IP multicast router it supports. The hosts are considered to lie *downstream* of the IGMP Relay device; the multicast router is *upstream*. The upstream link to the IP multicast router can be a frame relay link or a dial connection. For redundancy, an IGMP Relay device can be connected on upstream links to two IP multicast routers, a *primary* router and a *backup* router.

For example, Figure 9-2 shows an IGMP Relay device with downstream interfaces to three networks containing IGMP hosts. The IGMP Relay device also has an upstream interface to a primary IP multicast router and a second upstream interface to a backup IP multicast router on a dial-up line.

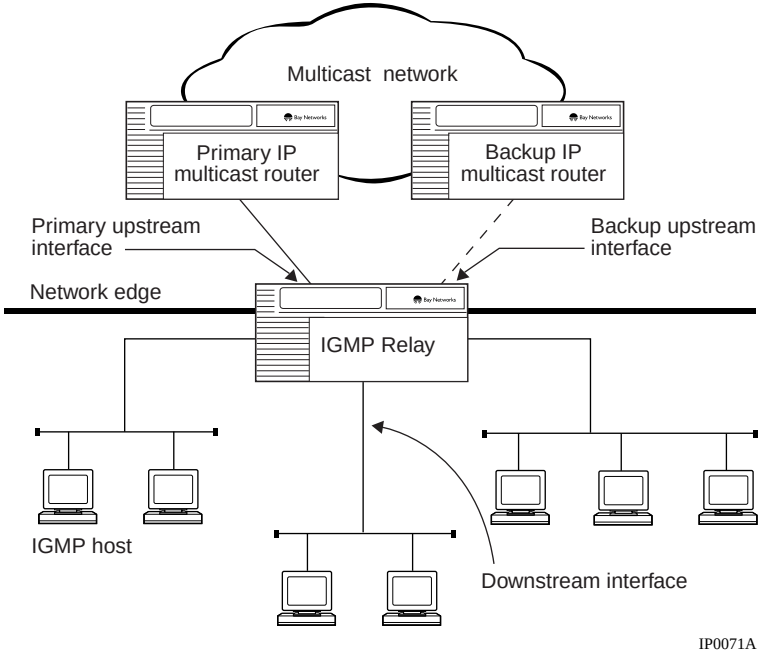

Figure 9-2. Multicast Network Topology with an IGMP Relay Device

How IGMP Relay Works

To an IGMP host on a directly attached network, the IGMP Relay device appears to be an IP multicast router. The host receives a host membership query from the IGMP Relay device and responds by sending an IGMP response. A host can also send the IGMP Relay device an unsolicited join message.

To IGMP running on the IP multicast router, the IGMP Relay device appears to be a locally attached host. IGMP on the IP multicast router sends IGMP host queries to the IGMP Relay device. IGMP Relay responds by forwarding -- relaying -- IGMP host reports and unsolicited join messages from its attached hosts.

In Figure 9-3, for example, the following events occur on the IGMP Relay device:

1. The IGMP Relay device sends IGMP host membership queries out the interfaces to LAN A, LAN B, and LAN C.
2. Host 1 on LAN A responds to the query by sending an IGMP host membership response to the IGMP Relay device.
3. IGMP Relay forwards the IGMP host membership response to the IP multicast router.

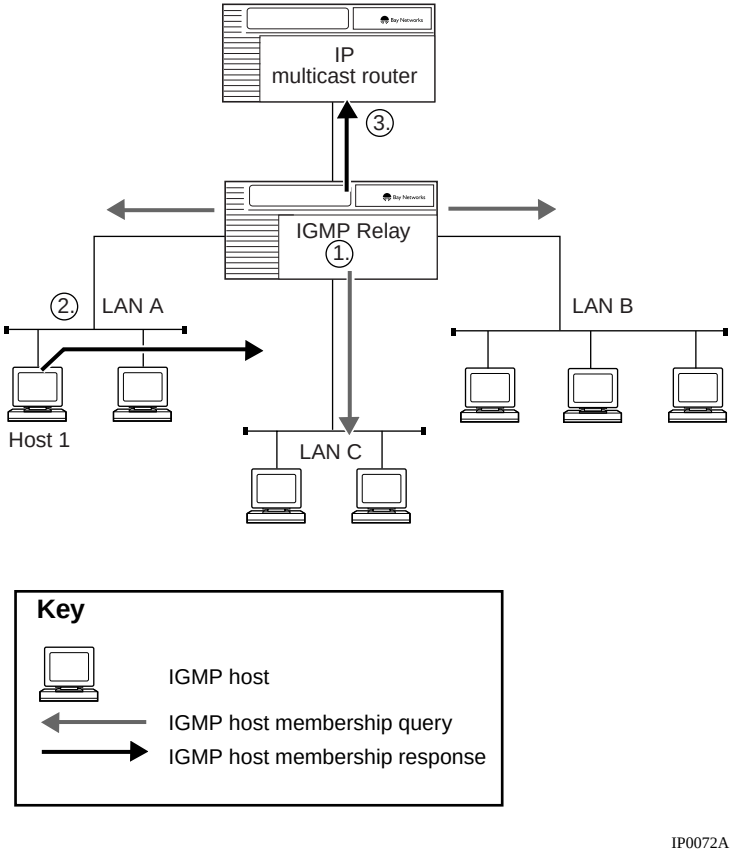

Figure 9-3. IGMP Relay Host Queries and Responses

In addition to soliciting multicast group membership information from directly attached networks, the IGMP Relay device relays multicast data packets generated by downstream hosts to the upstream IP multicast router. IGMP Relay also receives multicast data packets from the upstream multicast router and forwards them to the appropriate group members.

In Figure 9-4, for example, the following events occur:

1. Host 1 generates a datagram addressed to a multicast group and sends it upstream to the IGMP Relay device.
2. IGMP Relay forwards the multicast datagram upstream to the IP multicast router. IGMP Relay also forwards the packet on a downstream interface to a local group member.
3. The IP multicast router sends the datagram out the appropriate interface or interfaces to remote group members.

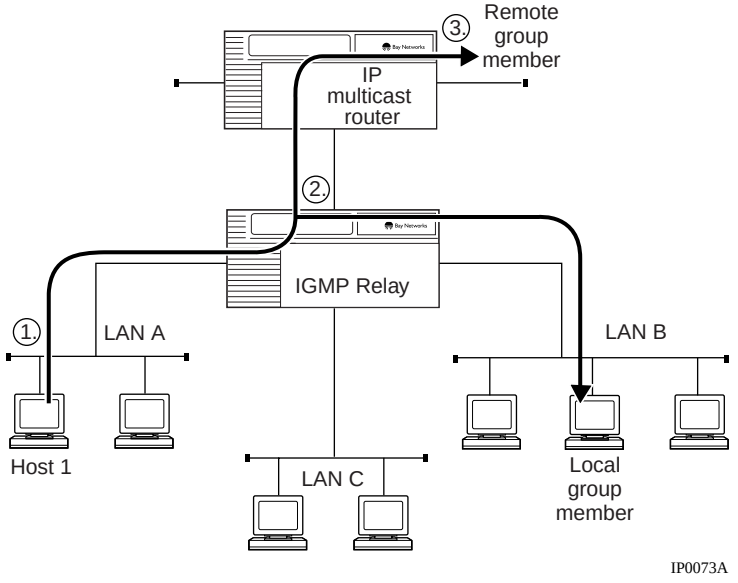

Figure 9-4. IGMP Relay and Upstream Multicast Data

A downstream host can also send an unsolicited join message to the IGMP Relay device. IGMP Relay forwards the message upstream to the IP multicast router.

In Figure 9-5, the following events occur:

1. A host on LAN B sends an unsolicited join message to the IGMP Relay device. IGMP Relay forwards the join message to the IP multicast router.
2. The IP multicast router receives a datagram addressed to the group that the host has joined.
3. The IP multicast router forwards the datagram downstream to IGMP Relay.
4. IGMP Relay determines that a member of the group resides on LAN B and forwards the datagram on the downstream interface to LAN B.

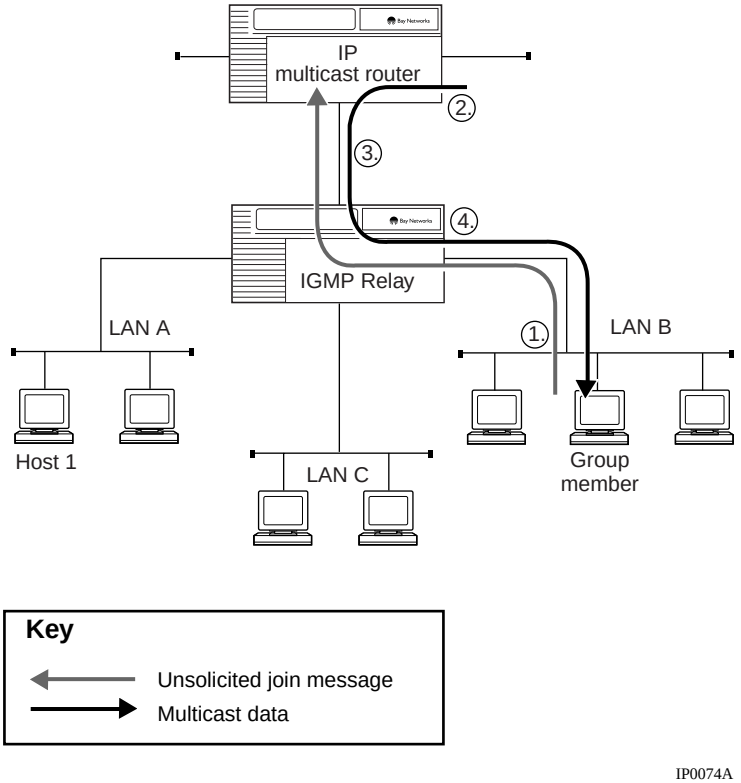

Figure 9-5. IGMP Relay and Downstream Multicast Data

Unicast Routing Protocols on the IGMP Relay Device

An IGMP Relay device does not run any multicast routing protocols.

You can configure a unicast routing protocol -- RIP or OSPF -- on the IGMP Relay device and add it to the upstream IP interface to the multicast router. The unicast protocol advertises the networks attached locally to the IGMP Relay device.

You can configure the IGMP Relay device with no routing protocols. In this case, you must statically insert routes to the IGMP Relay device's locally attached networks.

Routing Protocols on the Multicast Router

The IGMP Relay device supports the following types of multicast router:

- MOSPF boundary router. For information, see "Configuring MOSPF for Use with IGMP Relay" on page 9-18.
- DVMRP router. For information, see "Configuring a DVMRP Router for Use with IGMP Relay" on page 9-20.

Enabling and Disabling IGMP Relay Globally

By default, IGMP Relay is disabled on the router. You can use the BCC or Site Manager to enable and disable IGMP Relay globally.

Using the BCC

To enable or disable IGMP Relay on the router, navigate to the global IGMP prompt (for example, **box; ip; igmp**) and enter:

relay

The IGMP Relay prompt appears. IGMP Relay is now running and enabled globally.

To disable IGMP Relay, navigate to the IGMP Relay prompt and enter:

delete

For example, the following command sequence configures and enables IGMP Relay and then disables IGMP Relay:

```
igmp# relay
relay# delete
igmp#
```

Using Site Manager

To enable and disable IGMP Relay globally, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Global**.	The IGMP Global Configuration window opens.
5. Set the **Relay** parameter. Click on **Help** or see the parameter description on page A-19.	
6. Click on **Save**.	You return to the Configuration Manager window.

When you configure IGMP Relay globally, the IGMP Relay interface is configured as a downstream interface connecting the router to IGMP hosts. To change that value, see “Specifying the Relay Interface Type” on page 9-13.

Specifying a Timeout Value for Multicast Table Entries

By default, the timeout period for an entry in the multicast table is 60 seconds if there is no multicast data to refresh the entry.

You can use the BCC or Site Manager to specify a value for this parameter.

Using the BCC

To reset the timeout value for multicast table entries, navigate to the global IGMP Relay prompt (for example, **box; ip; igmp; relay**) and enter:

fwd-timeout *<seconds>*

seconds is the timeout period for an entry in the multicast table.

For example, the following command specifies a lifetime of 45 seconds for table entries:

```
relay# fwd-timeout 45
relay#
```

Using Site Manager

To specify a timeout value for multicast table entries, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Global**.	The IGMP Global Configuration window opens.
5. Set the **Relay Forwarding Timeout** parameter. Click on **Help** or see the parameter description on page A-20.	
6. Click on **Save**.	You return to the Configuration Manager window.

Configuring Upstream Data Forwarding

By default, an IGMP Relay device connected to a primary and backup IP multicast router uses the primary upstream interface when both the primary and the backup interfaces are active. When only one interface is active, the IGMP Relay device always uses that interface.

You can use the BCC or Site Manager to specify which interface to use for upstream data forwarding.

Using the BCC

To specify the upstream interfaces to use, navigate to the global IGMP Relay prompt (for example, **box; ip; igmp; relay**) and enter:

upstream-fwd *<option>*

option is one of the options listed in Table 9-1.

Table 9-1. IGMP Relay Forwarding Options

Option	Meaning
use-upstream-primary (default)	IGMP Relay uses the primary upstream interface only if both the primary interface and the backup interface are active.
use-upstream-backup	IGMP Relay uses the backup upstream interface only if both the primary interface and the backup interface are active.
both	IGMP Relay uses both the primary upstream interface and the backup upstream interface if both interfaces are active.

For example, the following command configures IGMP Relay to use both upstream interfaces if both interfaces are active:

```
relay# upstream-fwd both
relay#
```

Using Site Manager

To configure upstream data forwarding, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Global**.	The IGMP Global Configuration window opens.
5. Set the **Relay Upstream Forwarding** parameter. Click on **Help** or see the parameter description on page A-20.	
6. Click on **Save**.	You return to the Configuration Manager window.

Specifying the Relay Interface Type

The interface type parameter specifies that the IGMP Relay interface is configured on one of the following types of interface:

- A downstream interface connecting the IGMP Relay device to IGMP hosts (the default)
- An upstream interface connecting the IGMP Relay device to the primary IP multicast router
- An upstream interface connecting the IGMP Relay device to the backup IP multicast router

You can use the BCC or Site Manager to specify the interface type.

Using the BCC

To specify the IGMP Relay interface type, navigate to the IGMP Relay interface prompt (for example, **box; ethernet/2/2; ip/2.2.2.2/255.255.0.0; igmp; relay**) and enter:

type *<type>*

type is one of the values listed in Table 9-2.

Table 9-2. IGMP Relay Interface Types

Interface Type	Meaning
downstream (default)	Downstream interface connecting IGMP Relay to IGMP hosts
upstream-primary	Upstream interface connecting IGMP Relay to the primary IP multicast router
upstream-backup	Upstream interface connecting IGMP Relay to the backup IP multicast router

For example, the following command sequence invokes the IGMP prompt for IP interface 2.2.2.2 and specifies that the interface is the upstream interface to the primary IP multicast router:

```
igmp/2.2.2.2/1# relay
relay/2.2.2.2/1# type upstream-primary
relay/2.2.2.2/1#
```

Using Site Manager

To specify the IGMP Relay interface type, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Interfaces**.	The IGMP Interface Parameters window opens.
5. Set the **Relay Circuit Type** parameter. Click on **Help** or see the parameter description on page A-26.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Configuring Unsolicited Reports on an Upstream Interface

By default, an IGMP Relay device sends an unsolicited group report on the upstream interface. After an interval of 10 seconds, IGMP sends a second report.

Using the BCC or Site Manager, you can specify the interval between the first and second unsolicited reports or configure IGMP Relay to send one unsolicited report only.

Using the BCC

To configure unsolicited reports on an upstream interface, navigate to an IGMP Relay interface prompt (for example, **box; ethernet/2/2; ip/2.2.2.2/255.255.0.0; igmp; relay**) and enter:

report-interval *<interval>*

interval is one of the values described in Table 9-3.

Table 9-3. Unsolicited IGMP Report Interval

Value	Meaning
0	Configures IGMP Relay to send only one unsolicited group report on this interface
1-255 (Default is 10)	Configures the number of seconds that IGMP Relay waits to repeat the unsolicited report

For example, the following command configures IGMP Relay to repeat the unsolicited report after 30 seconds:

```
relay/2.2.2.2/1# report-interval 30
relay/2.2.2.2/1#
```

Using Site Manager

To configure unsolicited reports on an upstream interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Interfaces**.	The IGMP Interface Parameters window opens.
5. Set the **Relay Report Interval** parameter. Click on **Help** or see the parameter description on page A-26.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Configuring MOSPF for Use with IGMP Relay

An IGMP Relay device can provide host registration services for a multicast router configured as an MOSPF AS boundary router. To configure MOSPF for use with an IGMP Relay device, you must do the following:

- Configure the router as an MOSPF AS boundary router. For information about OSPF, see *Configuring IP, ARP, RIP, and OSPF Services.* For information about MOSPF, see Chapter 5, “Customizing OSPF Multicast Extensions.”
- Set the MOSPF Multicast Downstream IGMP Relay parameter to Enable. For information, see “Configuring Multicast-Capable External Routes” on page 5-10.
- Configure RIP globally on the MOSPF boundary router. For information about RIP, see *Configuring IP, ARP, RIP, and OSPF Services.*
- Add MOSPF and IGMP to each interface that connects the router to the multicasting domain.
- Add RIP, MOSPF, and IGMP to the downstream interface that connects the MOSPF boundary router to the IGMP Relay device. Note that MOSPF is configured on the multicast interface only. As a unicast device, IGMP Relay does not run MOSPF or any other multicast protocol on the upstream interface to the MOSPF boundary router.

Figure 9-6 shows how a Bay Networks MOSPF AS boundary router receives RIP and IGMP advertisements from IGMP Relay and injects them into the OSPF domain.

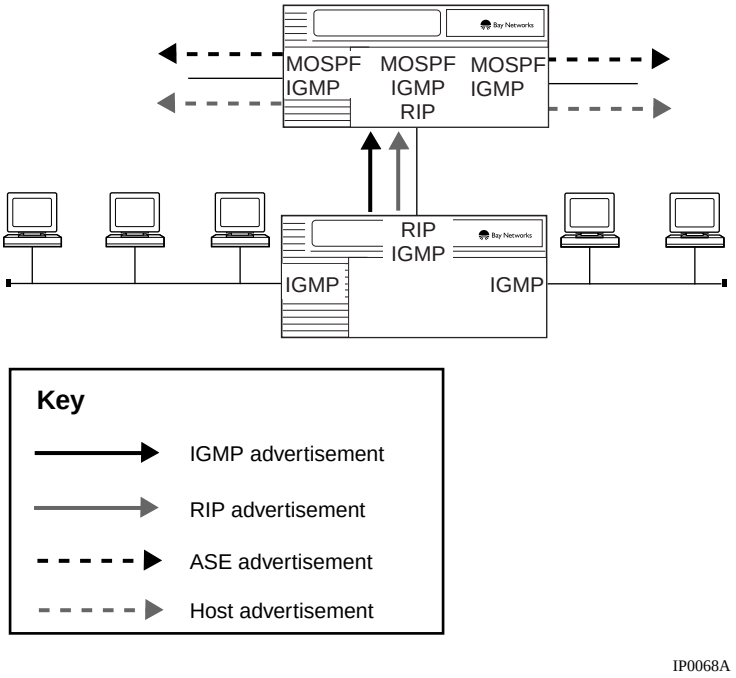

Figure 9-6. IGMP Relay Routing Protocols

The following events occur:

1. The MOSPF boundary router receives a RIP advertisement from IGMP Relay and injects it into the MOSPF domain as an AS external route.
2. The MOSPF boundary router receives IGMP host membership responses from IGMP Relay and floods group membership LSAs to other MOSPF routers in the domain.

Configuring a DVMRP Router for Use with IGMP Relay

An IGMP Relay device can provide host registration services for a multicast router running DVMRP. To configure a DVMRP router for use with an IGMP Relay device, you must do the following:

- If the IGMP Relay device is running RIP on its upstream IP interface, you must add RIP to the downstream IP interface on the multicast router. RIP advertises its locally attached networks to the multicast router. The multicast router stores the routes in its IP unicast routing table.
- If the IGMP Relay device is running OSPF on its upstream IP interface, you must add OSPF to the downstream IP interface on the multicast router. OSPF advertises its locally attached networks to the multicast router. The multicast router stores the routes in its IP unicast routing table.
- If the IGMP Relay device is running no unicast routing protocol to advertise routes to its locally attached networks, you must statically add the routes to the IP unicast routing table on the multicast router.

All three of these methods produce the same result: they ensure that the IP unicast routing table on the multicast router contains routes to the networks locally attached to the IGMP Relay device. However, DVMRP -- which builds its own routing table separate from the IP unicast routing table -- has no knowledge of the networks.

To make the routes known to DVMRP, you configure a DVMRP unicast accept policy that specifies the routes. DVMRP copies the routes from the IP unicast routing table and injects them into the DVMRP routing table.

For instructions, see “Configuring DVMRP Unicast Accept Route Policies” on page 4-69.

In Figure 9-7, for example:

1. The IGMP Relay device uses RIP to advertise net_1, net_2, and net_3 to the DVMRP multicast router. The RIP routes are stored in the IP unicast routing table.
2. The unicast accept route policy causes DVMRP to copy the three routes from the IP unicast routing table and inject them into the DVMRP routing table.

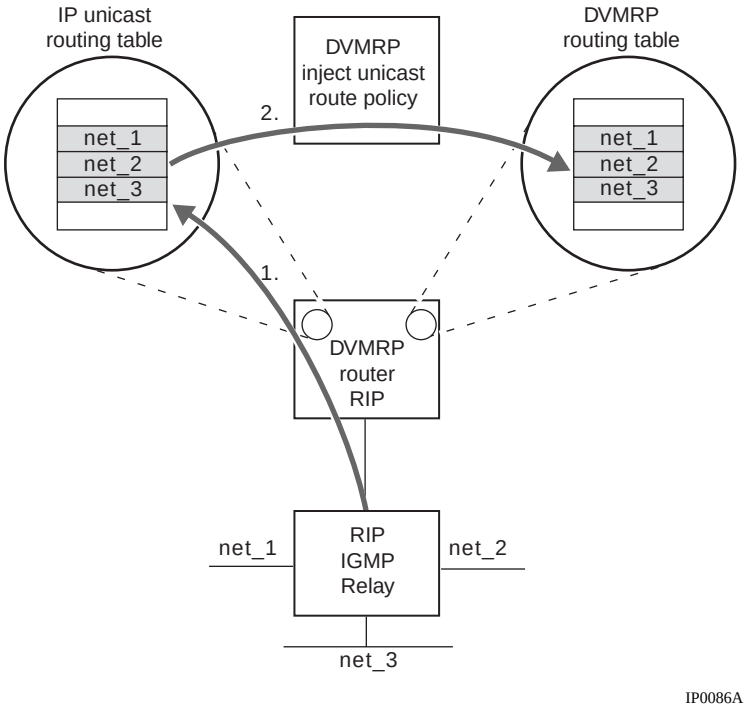

Figure 9-7. DVMRP Unicast Accept Route Policy

Configuring a Backup Multicast Router

IGMP Relay supports two types of backup configuration:

- Configurations that contain a primary and a backup multicast router
- Configurations that contain a primary and a backup IGMP Relay device

In Figure 9-8, for example, an IGMP Relay device has interfaces to two multicast routers. A leased line connects the IGMP Relay device to the primary multicast router. A dial-up line connects the IGMP Relay device to the backup multicast router.

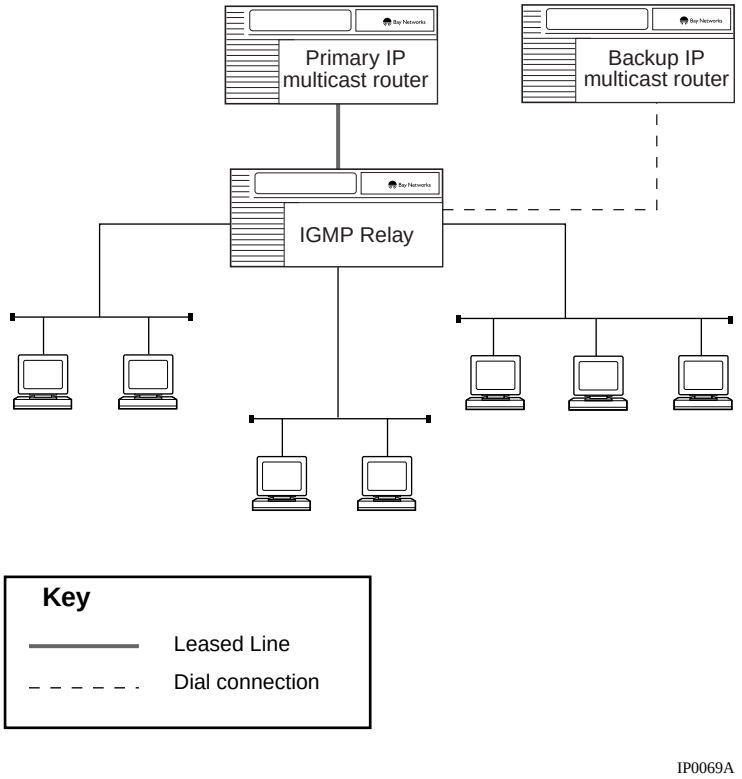

Figure 9-8. IGMP Relay with Primary and Backup Multicast Routers

For instructions on configuring a dial connection, see *Configuring Dial Services*.

Configuring IGMP Relay with Router Redundancy

IGMP Relay operates with Bay Networks router redundancy in hot standby mode.

Figure 9-9 shows a topology with two IGMP Relay devices configured for router redundancy. One of the IGMP Relay devices is configured as the primary device; the other is configured as the secondary device. When the primary device is active, it is responsible for all IGMP Relay functions as well as all routing features associated with the device. The secondary device remains in a passive mode with the protocols loaded but not actively processing or sending information.

If the secondary device determines that the primary device is inactive, the secondary device transitions to the active state, assuming all functions, including the IGMP Relay function. The original primary device transitions to the secondary state.

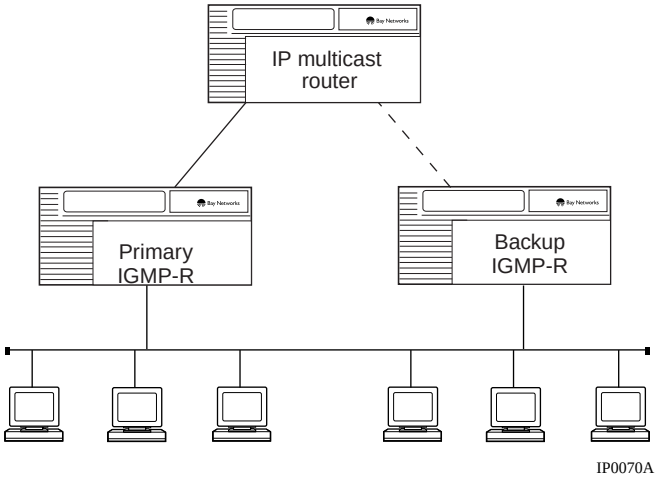

Figure 9-9. IGMP Relay with Router Redundancy

For information, see *Configuring Interface and Router Redundancy.*

Appendix A
Site Manager Parameters

This appendix contains the Site Manager parameter descriptions for multicast and multimedia services. You can display the same information using Site Manager online Help. This appendix contains the following information:

Topic	Page
DVMRP Parameters	A-2
IGMP Parameters	A-17
IP Configuration Parameters	A-26
Resource Manager Parameters	A-28
OSPF Parameters for Multicast Extensions	A-35
PIM Parameters	A-37
RSVP Parameters	A-54
Multicast Policy Parameters	A-59

For each parameter, this appendix provides the following information:

- Parameter name
- Configuration Manager menu path
- Default setting
- Valid parameter options
- Parameter function
- Instructions for setting the parameter
- Management information base (MIB) object ID

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, see *Using Technician Interface Software*.

Caution: The Technician Interface does not verify the validity of the parameter values that you enter. Entering an invalid value can corrupt your configuration.

DVMRP Parameters

Topic	Page
DVMRP Global Parameters	A-2
DVMRP Interface Parameters	A-7
DVMRP Tunnel Parameters	A-12

DVMRP Global Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IP > DVMRP > Global

Default: Enable

Options: Enable | Disable

Function: Enables and disables DVMRP support on the router.

Instructions: To disable DVMRP after you configure it on the router, specify Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.2

Parameter: Full Update Interval

Path:	Configuration Manager > Protocols > IP > DVMRP > Global
Default:	60
Options:	10 to 2000 (seconds)
Function:	Specifies in seconds how often routing messages containing complete routing tables are sent.
Instructions:	Determine the full-update interval that you require and specify a value from 10 through 2000 seconds (33 minutes, 20 seconds).
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.1.4

Parameter: Triggered Update Interval

Path:	Configuration Manager > Protocols > IP > DVMRP > Global
Default:	5
Options:	5 or more seconds
Function:	Specifies in seconds the maximum amount of time between triggered updates.
Instructions:	Triggered updates are sent between full updates. Issuing a full update restarts the triggered update timer. Therefore, the triggered update interval you specify must be shorter than the full update interval you specified with the Full Update Interval parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.1.5

Parameter: Leaf Timeout

Path:	Configuration Manager > Protocols > IP > DVMRP > Global
Default:	200
Options:	25 to 4000 (seconds)
Function:	Specifies in seconds a value for the leaf timeout timer.
Instructions:	Determine the timer interval you require and specify a value from 25 through 4000 seconds (1 hour, 6 minutes, and 40 seconds).
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.1.6

Parameter:	**Neighbor Timeout**
Path:	Configuration Manager > Protocols > IP > DVMRP > Global
Default:	140
Options:	40 to 8000 (seconds)
Function:	Specifies in seconds how long a connection with a router neighbor is considered active without receiving a subsequent probe or report from the neighbor.
Instructions:	Determine a neighbor timeout period and specify a value from 40 through 8000 seconds (2 hours, 13 minutes, and 20 seconds).
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.1.7

Parameter:	**Route Expiration Timeout**
Path:	Configuration Manager > Protocols > IP > DVMRP > Global
Default:	200
Options:	20 to 4000 (seconds)
Function:	Specifies in seconds how long a route is considered valid without the receipt of a subsequent update indicating that the route is reachable. This value represents the duration of time that this route will be used. Upon expiration of this timer, this route is advertised as unreachable until it is refreshed or deleted.
Instructions:	Enter a value from 20 through 4000 seconds (1 hour, 6 minutes, and 40 seconds) that represents the duration of time this route will be used without being refreshed.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.1.8

Parameter: Garbage Timeout

Path: Configuration Manager > Protocols > IP > DVMRP > Global

Default: 340

Options: 40 to 8000 (seconds)

Function: Specifies in seconds the duration of time that this route will be included in routing updates without the receipt of a subsequent update indicating that the route is reachable. The difference between this value and the Route Expiration Timeout value represents the duration of time that the route will be advertised as unreachable without subsequent refreshment.

Instructions: Enter a value from 40 through 8000 seconds (2 hours, 13 minutes, and 20 seconds) that is greater than the value you specified for Route Expiration Timeout to allow for sufficient time for the route to be advertised as unreachable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.9

Parameter: Estimated Routes

Path: Configuration Manager > Protocols > IP > DVMRP > Global

Default: 25

Options: An integer of 10 or greater

Function: Specifies the estimated number of routes in the routing table.

Instructions: Enter a value that the router can use for preallocating routing tables. For an MBone implementation, a value of 3000 or higher is recommended. Note that routes are kept on a per-source-network basis, independent of multicast groups. This number must include a route for every network that is local to a circuit configured for multicasting. This allows the router to utilize memory efficiently. Exceeding this size during router operation will not cause an error but may cause the router to consume more memory than is required.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.10

Parameter: Neighbor Probe Interval

Path: Configuration Manager > Protocols > IP > DVMRP > Global
Default: 10
Options: 5 to 30 (seconds)
Function: Specifies how often DVMRP should send a probe on interfaces from which no neighbors have been heard.
Instructions: If the neighbor is running DVMRP *mrouted*, ensure that the probe interval value matches the value used by the neighbor.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.11

Parameter: Route Switch Timeout

Path: Configuration Manager > Protocols > IP > DVMRP > Global
Default: 140
Options: 20 to 2000 (seconds)
Function: Specifies in seconds how long DVMRP should wait, without receiving a subsequent route update from the original neighbor, before switching to a different neighbor advertising equal cost for this route.
Instructions: Enter a value from 20 through 2000 seconds (33 minutes, 20 seconds). If the neighbor is running DVMRP *mrouted*, you should accept the default value, 140 seconds.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.12

Parameter: Debug Level

Path: Configuration Manager > Protocols > IP > DVMRP > Global
Default: 0
Options: 0 or a debug level
Function: Turns the DVMRP log on or off for DVMRP debugging messages and specifies the level of debug messages.
Instructions: By default (0), the log is turned off. Specify a level only when directed by Customer Support personnel to investigate a problem.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.14

Parameter: **Pruning Enable**

Path: Configuration Manager > Protocols > IP > DVMRP > Global

Default: Enable

Options: Enable │ Disable

Function: Enables or disables pruning functionality on the router.

Instructions: DVMRP performs route pruning by default. If you want to disable this function on the router, select Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.15

Parameter: **Max Routes**

Path: Configuration Manager > Protocols > IP > DVMRP > Global

Default: 0

Options: 0 or any integer

Function: Specifies the number of routes that DVMRP can learn per slot. This parameter limits the number of routes that can be stored in the routing table.

Instructions: If you want DVMRP to store all learned routes in the routing table, use the default, 0. If you specify a maximum number of routes, you must include a route for every local network that has a circuit configured for multicasting.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.17

DVMRP Interface Parameters

Parameter: **Enable**

Path: Configuration Manager > Protocols > IP > DVMRP > Circuit

Default: Enable

Options: Enable │ Disable

Function: Enables or disables DVMRP on this circuit.

Instructions: If you have configured DVMRP on this circuit, enter Disable to disable it.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.2

Parameter: Route Enable

Path: Configuration Manager > Protocols > IP > DVMRP > Circuit

Default: Enable

Options: Enable │ Disable

Function: Enables or disables this circuit for routing.

Instructions: Specify Enable if you want this circuit to be used to propagate routing information, and if you want information about the source network associated with this circuit incorporated into routing updates. Specify Enable if you want multicast datagrams to be forwarded on this circuit in "native mode" -- that is, as multicast datagrams. You can configure tunnels on this circuit.

Specify Disable if you want this circuit to exist only to support unicast tunnels. If you specify Disable, all other DVMRP circuit parameters are ignored. The source network associated with this circuit is not incorporated into the routing updates.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.5

Parameter: Metric

Path: Configuration Manager > Protocols > IP > DVMRP > Circuit

Default: 1

Options: 1 to 31

Function: Specifies the cost of this interface.

Instructions: Determine the cost that you want to assign to this hop and enter a value. Bay Networks recommends the following values: for a LAN or tunnel across a single LAN: 1; for a multihop tunnel: 2 or 3; for a serial line or tunnel across a serial link: 1; for a backup tunnel: the primary tunnel metric + 1.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.6

Parameter: Threshold

Path: Configuration Manager > Protocols > IP > DVMRP > Circuit

Default: 1

Options: 1 to 254

Function: Specifies (in hops) a TTL value for the interface. This value is the minimum IP TTL required for a multicast datagram to be forwarded out this interface.

Instructions: Use this parameter to control the scope of the datagrams. If the IP TTL is less than the threshold value you specify, the router drops the datagram.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.7

Parameter: Forward Cache Size

Path: Configuration Manager > Protocols > IP > DVMRP > Circuit

Default: 32

Options: 32 to 512

Function: Specifies the maximum number of entries allowed in the forwarding table associated with this interface.

Instructions: When configuring a cache size, you must also keep in mind the TTL value for entries. If you specify a large cache size, a larger TTL value is recommended. For a smaller cache, a shorter TTL for cache entries is recommended.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.14

Parameter: Forward Cache TTL

Path: Configuration Manager > Protocols > IP > DVMRP > Circuit

Default: 7200

Options: 300 to 86,400 (seconds)

Function: Specifies in seconds the TTL for an entry in the forwarding table.

Instructions: Enter a value from 300 seconds (5 minutes) through 86,400 seconds (24 hours). If the neighbor is running DVMRP *mrouted*, Bay Networks recommends a TTL value of 300 seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.15

Parameter: Advertise Self

Path: Configuration Manager > Protocols > IP > DVMRP > Circuit
Default: Advertise
Options: Advertise | Do Not Advertise
Function: Specifies whether the router advertises its own local networks over this interface.
Instructions: If you do not want routes advertised over a particular interface, set this parameter to Do Not Advertise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.16

Parameter: Supply Default Route

Path: Configuration Manager > Protocols > IP > DVMRP > Circuit
Default: Enable
Options: Enable | Disable | Generate
Function: Specifies whether to enable or disable the default route (0.0.0.0), or to generate a default route on this interface.
Instructions: Enable this feature if you want DVMRP to advertise a default route on this interface. To generate a default route, specify Generate.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.24

Parameter: Listen Default Route

Path: Configuration Manager > Protocols > IP > DVMRP > Circuit
Default: Enable
Options: Enable | Disable
Function: Receives the default route (0.0.0.0) on this interface.
Instructions: Enable this feature if you want DVMRP to listen for a default route on this interface.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.25

Parameter: Report Depend Probe

Path:	Configuration Manager > Protocols > IP > DVMRP > Circuit
Default:	Disable
Options:	Enable | Disable
Function:	Specifies the conditions under which DVMRP accepts a route report. According to the protocol, DVMRP must send a probe packet before sending the route report packet to its neighbors. Some vendor implementations, however, do not send probes before sending reports.
Instructions:	By default, DVMRP processes all received route reports. Enable this feature if you want DVMRP to process only routes received from neighbors that send probe packets.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.2.1.26

Parameter: Prune Life Time

Path:	Configuration Manager > Protocols > IP > DVMRP > Circuit
Default:	7200
Options:	0 to 86,400 (seconds)
Function:	Specifies in seconds the lifetime of a prune message that DVMRP sends to a neighbor on this interface.
Instructions:	Enter a value from 0 through 86,400 seconds (24 hours). The default, 7200 seconds, is equal to 2 hours.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.2.1.27

DVMRP Tunnel Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IP > DVMRP > Tunnel
Default: Enable
Options: Enable │ Disable
Function: Enables or disables this tunnel.
Instructions: Specify Disable to disable the tunnel.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.2

Parameter: Encapsulation Mode

Path: Configuration Manager > Protocols > IP > DVMRP > Tunnel
Default: IP Datagram
Options: IP Datagram │ LSSR Option
Function: Specifies whether tunneled datagrams are encapsulated within an IP datagram or loosely encapsulated using the LSSR option.
Instructions: See RFC 1075 for information about the LSSR option, which is provided for backward compatibility.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.6

Parameter: Metric

Path: Configuration Manager > Protocols > IP > DVMRP > Tunnel
Default: 1
Options: 1 to 31
Function: Specifies the cost of this tunnel.
Instructions: Determine the cost that you want to assign to this tunnel and enter a value. Bay Networks recommends the following values: for a LAN or tunnel across a single LAN: 1; for a multihop tunnel: 2 or 3; for a serial link or tunnel across a serial link: 1; for a backup tunnel: the primary tunnel metric + 1.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.7

Parameter: Threshold

Path: Configuration Manager > Protocols > IP > DVMRP > Tunnel

Default: 1

Options: 1 to 254

Function: Specifies in hops a TTL value for the tunnel. This value is the minimum IP TTL required for a multicast datagram to be forwarded out this tunnel.

Instructions: Use this parameter to control the scope of the datagrams. If the IP TTL is less than the threshold value you specify, the router drops the datagram.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.8

Parameter: Forward Cache Size

Path: Configuration Manager > Protocols > IP > DVMRP > Tunnel

Default: 32

Options: 32 to 512

Function: Specifies the maximum number of entries allowed in the forwarding table associated with this tunnel interface.

Instructions: When configuring a cache size, you must also keep in mind the TTL value for entries. If you specify a large cache size, a larger TTL value is recommended. For a smaller cache, a shorter TTL for cache entries is recommended.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.16

Parameter: Forward Cache TTL (Secs)

Path: Configuration Manager > Protocols > IP > DVMRP > Tunnel

Default: 7200

Options: 300 to 86,400 (seconds)

Function: Specifies in seconds the TTL for an entry in the forwarding table.

Instructions: Select an appropriate value for your configuration, from 300 seconds (5 minutes) through 86,400 seconds (24 hours).

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.17

Parameter: Route Supply

Path: Configuration Manager > Protocols > IP > DVMRP > Tunnel
Default: Enable
Options: Enable │ Disable │ Generate
Function: Supplies the default route (0.0.0.0) on this interface.
Instructions: Enable this feature if you want DVMRP to advertise a default route on this tunnel interface. To generate a default route, specify Generate.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.25

Parameter: Route Listen

Path: Configuration Manager > Protocols > IP > DVMRP > Tunnel
Default: Enable
Options: Enable │ Disable
Function: Receives the default route (0.0.0.0) on this interface.
Instructions: Enable this feature if you want DVMRP to listen for a default route on this interface.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.26

Parameter: Control Message Mode

Path: Configuration Manager > Protocols > IP > DVMRP > Tunnel
Default: Noencaps
Options: Encaps │ Noencaps
Function: Specifies the encapsulation mode for IGMP control packets.

Noencaps causes IGMP to send control messages in regular IGMP packets with the IP protocol type set to IP_PROTOCOL_IGMP.

Encaps causes IGMP to encapsulate control messages inside IP packets with the IP protocol type set to IP_PROTOCOL_IPINIP.

All DVMRP messages sent across tunnels will be encapsulated in the same way as data packets in this mode.

Instructions: Select an encapsulation mode for control messages.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.27

Parameter: Report Depend Probe

Path: Configuration Manager > Protocols > IP > DVMRP > Tunnel

Default: Disable

Options: Enable │ Disable

Function: Specifies the conditions under which DVMRP accepts a route report. According to the protocol, DVMRP must send a probe packet before sending the route report packet to its neighbors. Some vendor implementations, however, do not send probes before sending reports.

Instructions: By default, DVMRP processes all received route reports. Enable this feature if you want DVMRP to process only routes received from neighbors that have sent probe packets in accordance with the protocol.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.28

Parameter: Prune Life Time

Path: Configuration Manager > Protocols > IP > DVMRP > Tunnel

Default: 7200

Options: 0 to 86,400 (seconds)

Function: Specifies (in seconds) the lifetime of a prune message that DVMRP sends to a neighbor on this tunnel.

Instructions: Set this parameter from 0 through 86,400 seconds (24 hours). The default, 7200 seconds, is equal to 2 hours.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.29

Parameter:	**Local IP Address**
Path:	Configuration Manager > Protocols > IP > DVMRP > Tunnel > **Add**
Default:	Null
Options:	The unicast IP address of an interface on a circuit supporting multicasting on the local router
Function:	Identifies the local end of the tunnel. To identify a unicast tunnel, you must supply the unicast IP addresses of both ends of the tunnel: the local interface and the remote interface.
Instructions:	Use this parameter to enter the local IP address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.3.1.4

Parameter:	**Remote IP Address**
Path:	Configuration Manager > Protocols > IP > DVMRP > Tunnel > **Add**
Default:	Null
Options:	The unicast IP address of an interface supporting multicasting on a neighboring router
Function:	Identifies the remote end of the tunnel. To identify a unicast tunnel, you must supply the unicast IP addresses of both ends of the tunnel: the local interface and the remote interface.
Instructions:	Use this parameter to enter the remote IP address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.3.1.5

IGMP Parameters

This section describes IGMP global configuration, static host, and interface parameters.

IGMP Global Configuration Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default: Enable
Options: Enable │ Disable
Function: Enables or disables this IGMP record.
Instructions: If you configured IGMP on this router, use this parameter to disable it.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.2

Parameter: Estimated Groups

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default: 20
Options: 5 to 65,535
Function: Specifies the estimated number of multicast groups that will be simultaneously active for this router. This estimate allows the router to use memory efficiently. Exceeding this size during router operation will not cause an error but may cause the router to consume more memory than required. The following groups are not maintained by IGMP; you do not need to include them in the count: 224.0.0.1, 224.0.0.4, 224.0.0.5, and 224.0.0.6.
Instructions: Determine the approximate number of groups and enter the value.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.4

Parameter: Version Threshold Time

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default: 540
Options: 1 to 65,535 (seconds)
Function: Specifies the number of seconds that can elapse after IGMP detects a Version 1 query before IGMP tries to become the designated querier.
Instructions: Enter a value from 1 through 65,535 seconds (18 hours, 12 minutes, and 15 seconds). The value that you specify should be greater than the Version 1 query rate of all IGMP speakers on all networks directly connected to the router.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.5

Parameter: Join Ack Enable

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default: Disable
Options: Enable │ Disable
Function: Indicates whether IGMP should send an immediate response (in the form of a query) to the group associated with this IGMP membership report.
Instructions: Set this parameter as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.7

Parameter: Forward Cache Limit

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default: 512
Options: 64 to 65,535
Function: Specifies the maximum number of MTM forwarding cache entries.
Instructions: Set this parameter as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.8

Parameter: Debug

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global

Default: None

Options: See instructions.

Function: Causes IGMP to generate the specified log messages.

Instructions: Click on Values and select the types of log messages that you want IGMP to generate. The Debug field displays the following bitmasks for each type of message:

0x00000001 for received IGMP join/leave packets
0x00000002 for sent IGMP messages
0x00000004 for received multicast protocol messages
0x00000008 for MTRACE log messages
0x00000010 for configuration log messages
0x00000020 for interaction with multicast protocols
0x00000040 for interaction with RSVP
0x00000080 for MTM forwarding cache log messages
0x00000100 for IGMP-R log messages

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.6

Parameter: Relay

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global

Default: Disable

Options: Enable │ Disable

Function: Enables and disables IGMP Relay.

Instructions: Set the parameter as required.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.10

Parameter: Nonlocal Reports

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default: Ignore
Options: Ignore │ Accept
Function: Controls whether IGMP accepts or ignores leave and join messages from a nonlocal network.
Instructions: Set the parameter as required by your configuration.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.9

Parameter: Relay Forwarding Timeout

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default: 60
Options: Any integer
Function: Sets the lifetime in seconds of IGMP Relay Multicast Table Manager forwarding entries.
Instructions: Set the timer as required by your configuration.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.11

Parameter: Relay Upstream Forwarding

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default: Primary
Options: Primary │ Backup │ Both
Function: Specifies whether multicast data is forwarded from the IGMP Relay device onto the primary upstream interface, the backup interface, or both when both interfaces are active.
Instructions: Select an option as required by your configuration.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.12

IGMP Static Host Parameters

Parameter: Group Address

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Static Groups

Default: None

Options: A multicast address

Function: Specifies the multicast address for the group of which the host is a member. Use the static group parameters to manually register the network on which the multicast group member resides.

Instructions: Enter the multicast address for the group.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.4.1.3

Parameter: Prefix Length

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Static Groups

Default: None

Options: The length of the address prefix

Function: Specifies the length of the prefix of the multicast group address. Use the static group parameters to manually register the network on which the multicast group member resides.

Instructions: Enter a value from 0 through 32.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.4.1.4

Parameter:	**Circuit Name**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Static Groups
Default:	None
Options:	A circuit name
Function:	Specifies the circuit name for the local network on which the group member resides. Use the static group parameters to manually register the network on which the multicast group member resides.
Instructions:	Click on Values and select the circuit name from the list.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.4.1.2

IGMP Interface Parameters

Parameter:	**Enable**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default:	Enable
Options:	Enable | Disable
Function:	Indicates whether this IGMP interface record is enabled or disabled.
Instructions:	If you configured IGMP on this interface, use this parameter to disable it.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.2.1.2

Parameter: Interface Query Rate

Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default:	120
Options:	0 to 4096 (seconds)
Function:	Specifies how often the router sends group membership queries on the interface.
Instructions:	If there are no multicast hosts on this circuit, set the parameter to 0 to disable queries. Specifying 0 affects queries only. The router still forwards multicast datagrams on this circuit. If another IGMP router on this network has assumed the query role, this router will not send queries unless it has not heard of any queries within the number of seconds specified by the Designated Router Timeout parameter. The maximum value, 4096 seconds, is equal to 1 hour, 8 minutes, and 16 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.2.1.5

Parameter: Interface Membership Timeout

Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default:	260
Options:	30 to 8192 (seconds)
Function:	Specifies in seconds the amount of time that a local group membership is valid without the receipt of a subsequent report for that group.
Instructions:	The suggested value is (2 * Interface Query Rate) + 20. The maximum value, 8192 seconds, is equal to 2 hours, 16 minutes, and 32 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.2.1.6

Parameter: Designated Router Timeout

Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default:	140
Options:	10 to 8192 (seconds)
Function:	Specifies in seconds the amount of time that can elapse after the last host query message before the IGMP designated router is considered down.
Instructions:	Set an approximate value. This value should be greater than the query rate of all IGMP routers on the network. The maximum value, 8192 seconds, is equal to 2 hours, 16 minutes, and 32 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.2.1.7

Parameter: Max Host Response Time

Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default:	100
Options:	1 to 100 (tenths of a second)
Function:	Specifies, in tenths of a second, a maximum value for the amount of time that a host must wait before responding to a query. IGMP places this value in the code field of an IGMP query.
Instructions:	Specify a maximum response time for this interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.2.1.15

Parameter: Mtrace Entry Lifetime

Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default:	30
Options:	30 to 8192 (seconds)
Function:	Specifies in seconds the amount of time that a router should keep a forwarding cache entry that was created specifically for Mtrace.
Instructions:	Specify an Mtrace lifetime value for the interface. The maximum value, 8192 seconds, is equal to 2 hours, 16 minutes, and 32 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.2.1.18

Parameter: Query Suppression

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces

Default: No

Options: Yes | No

Function: Specifies whether IGMP queries are suppressed on this interface.

Instructions: In the Bay Networks multicast implementation, configuring IGMP on an interface means two things: (1) the interface is used for forwarding multicast traffic and (2) IGMP is running on the interface. Therefore, on some interfaces -- for example, point-to-point or nonbroadcast -- even though there is no need to run the IGMP protocol, IGMP must still be configured. On such interfaces, you can disable the sending of IGMP queries.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.25

Parameter: Static Forward Cache Lifetime

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces

Default: 216

Options: 80 to 7200 (seconds)

Function: If the IGMP static forwarding policy is set to Static to Dynamic (static inbound and multicast protocol outbound), specifies the number of seconds that the Multicast Table Manager cache entries will be alive for, even if traffic is not present.

Instructions: Set this value based on the multicast protocol that is configured on the outbound interface: a typical value for DVMRP is 7200 seconds (2 hours) and for MOSPF, 600 seconds (10 minutes).

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.28

Parameter: Relay Circuit Type

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces

Default: Downstream

Options: Primary │ Backup │ Downstream

Function: Specifies whether the IGMP circuit is configured as the primary upstream circuit, the backup upstream circuit, or a downstream circuit.

Instructions: You can configure only one primary and one backup upstream circuit on the router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.23

Parameter: Relay Report Interval

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces

Default: 10

Options: 0 to any integer

Function: Specifies the interval (in seconds) between the initial group membership report on an IGMP-R primary or backup circuit and a repetition of that report.

Instructions: Using 0 causes IGMP-R to send an unsolicited group report once only.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.24

IP Configuration Parameters

Parameter: IP Address

Path: Select IP from the Select Protocols window and click on OK.

Default: None

Options: 0.0.0.0 or any valid IP address

Function: Assigns a 32-bit IP address to the interface.

Instructions: Enter the IP address of the interface in dotted-decimal notation. Enter 0.0.0.0 to configure an unnumbered interface on the circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.1.4

Parameter: Subnet Mask

Path: Select IP from the Select Protocols window and click on OK.

Default: None

Options: The Configuration Manager automatically calculates an appropriate subnet mask, depending on the class of the network to which the interface connects. However, you can change the subnet mask using this parameter.

Function: Specifies the network and subnetwork portion of the 32-bit IP address.

Instructions: Either accept the assigned subnet mask or enter another subnet mask in dotted-decimal notation. Enter 0.0.0.0 if you are configuring an unnumbered interface on the circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.1.6

Parameter: Transmit Bcast Addr

Path: Select IP from the Select Protocols window and click on OK.

Default: 0.0.0.0

Options: 0.0.0.0 or any valid IP broadcast address

Function: Specifies the broadcast address that this IP subnet uses to broadcast packets. Accepting 0.0.0.0 for this parameter specifies that the IP router will use a broadcast address with a host portion of all 1s. Accepting 0.0.0.0 does not configure the router to use the address 0.0.0.0 to broadcast packets. For example, if you have IP address 123.1.1.1 and a subnet mask of 255.255.255.0, accepting the default value 0.0.0.0 configures the IP router to use the address 123.1.1.255 to broadcast packets. To set the explicit broadcast address of all 1s, enter 255.255.255.255 for this parameter.

Instructions: Accept the default, 0.0.0.0, unless the calculated broadcast address (host portion) of all 1s is not adequate. If this is the case, then enter the appropriate IP broadcast address in dotted-decimal notation. If you set the IP Address parameter to 0.0.0.0 (to configure an unnumbered interface), Site Manager automatically sets this parameter to 255.255.255.255.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.1.8

Parameter: **UnNumbered Assoc Address**

Path: Select IP from the Select Protocols window and click on OK.

Default: None

Options: Any valid IP address

Function: Specifies an address that IP uses when sourcing a packet. RIP uses this address to make decisions about advertising subnets over the unnumbered interface. RIP advertises subnets over the unnumbered interface if the subnets have the same mask as the associated address.

Instructions: Specify the address of any numbered interface on the router. If you are running RIP over the unnumbered interface and if you are using a subnet address as the associated address, the local and remote associated addresses should have the same network number. If you configure local and remote associated addresses using different network numbers, you must use RIP2 mode.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.1.110

Resource Manager Parameters

Parameter: **Estimated Bandwidth**

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: 0

Options: 0 to 214,748,364

Function: Specifies the estimated usable bandwidth for this line in bits per second.

Instructions: Enter the estimated total bandwidth for this line in bits per second. To enable line resource management, enter a value greater than 0. For point-to-point lines, you can usually enter the total line speed.

For an Ethernet line, you must estimate a value, because shared-media lines may not have all of the bandwidth available. You can base the estimate on line statistics, the number of connected workstations, or other site-specific information.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.3

Parameter: Reservable Bandwidth

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: 0

Options: 0 to 214,748,364

Function: Specifies the reservable bandwidth for this line in bits per second.

Instructions: To enable reservable resources, enter the portion of this line's bandwidth that you want to make available for RSVP requests for guaranteed service. The value must be greater than 0 and less than the value of the Estimated Bandwidth parameter. Do not make all available bandwidth reservable; leave at least 15 percent for network management and routing protocols.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.4

Parameter: Traffic Queuing Algorithm

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: Priority

Options: None | Priority

Function: Specifies the queuing algorithm for all reserved traffic.

Instructions: Select None to use best-effort scheduling. Use best-effort scheduling if you want to use the Resource Reservation Protocol (RSVP) to control admission of flows to the network, but do not want to explicitly schedule each flow's packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.5

Parameter: Policing Algorithm

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: Leaky Bucket

Options: None | Leaky Bucket

Function: Specifies whether or not to use the leaky bucket policing algorithm for reserved traffic. With leaky bucket policing, the Resource Manager makes sure that all RSVP packets using reserved bandwidth follow the flowspec that appears in the RSVP connect request. The Resource Manager discards any packets that do not adhere to the flowspec. Note that such policing requires additional processing by the router.

Instructions: Select None to bypass policing if an upstream router is policing traffic, or if the applications generating the reserved traffic consistently adhere to the flowspec and do not require policing.

Select Leaky Bucket to apply a leaky bucket policing algorithm to reserved traffic.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.6

Parameter: Bandwidth Interval (Secs)

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: 10

Options: 1 to 214,748,364 (seconds)

Function: Specifies in seconds the interval over which the Resource Manager measures instantaneous bandwidth.

Instructions: Enter a time interval if the default value of 10 seconds is not sufficient. The maximum value, 214,748,364 seconds, is almost equal to 7 years.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.7

Parameter: **Inflate Reservations Percentage**

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: 0

Options: 0 to 100

Function: Specifies whether the Resource Manager adds a safety buffer to each RSVP reservation on this line by increasing bandwidth requests by a specified percentage.

Instructions: To inflate reservations made on this line, enter a percent value to increase each bandwidth request. Increase the value of this parameter if you notice that the Resource Manager is discarding packets because applications generating reserved traffic are exceeding their flowspecs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.8

Parameter: **Unreserved Policing Algorithm**

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: Queue Limit

Options: Queue Limit | Leaky Bucket

Function: Specifies the policing algorithm for unreserved traffic.

Instructions: Select the Queue Limit option to restrict the number of buffers (packets) of unreserved traffic that the Resource Manager queues. This method of policing enables unreserved traffic to use available reserved bandwidth. The Unreserved Queue Length parameter specifies the maximum number of packets in the queue.

Select the Leaky Bucket option to cause the router to actively police the unreserved traffic based on the unreserved bandwidth. This method does not allow unreserved traffic to take advantage of available reserved bandwidth.

If you enable priority queuing for this line, the router uses the priority queue parameters to perform Queue Limit policing. See *Configuring Traffic Filters and Protocol Prioritization* for information about priority queue parameters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.9

Parameter: **Unreserved Queue Length**

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: 20

Options: 0 to 214,748,364 packets (limited by available buffers)

Function: If the Unreserved Policing Algorithm parameter is set to Queue Limit, this parameter specifies the maximum number of unreserved (best-effort) packets to be held in queue for transmission.

After the queue length reaches this value, the router discards best-effort traffic when congestion occurs.

Priority queuing limits, if configured, override the value of this parameter.

Instructions: Change this value to adjust the queue length limit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.10

Parameter: **Multiline Select Algorithm**

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: First Fit

Options: First Fit | Round Robin

Function: Specifies how the Resource Manager selects which line to use for a new resource request, if you have the Resource Manager configured on a multiline circuit.

Instructions: Set this parameter only if you configured the Resource Manager on a multiline circuit.

Select First Fit to always use the first available line that can service reserved traffic requests. Select Round Robin to rotate the use of lines available to service requests. All lines for a circuit must use the same algorithm. If any one line on a circuit specifies First Fit, all lines use the first fit algorithm.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.11

Parameter: Multiline Threshold Bandwidth

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: 0

Options: 0 to 214,748,364

Function: Specifies how the first fit algorithm works, providing you set the Multiline Select Algorithm parameter to First Fit. If you accept the default value, the Resource Manager uses the simple first fit algorithm. If you select a value greater than 0, the Resource Manager still uses the first available line with reservable bandwidth to service requests, but moves to the next available line after reaching the configured threshold. When all lines are at their thresholds, the Resource Manager resumes using the simple first fit algorithm.

Instructions: Set this parameter only if you configured the Resource Manager on a multiline circuit and set the Multiline Select Algorithm parameter to First Fit.

Accept the default or enter a number less than the value of the Reservable Bandwidth parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.12

Parameter: Reservation Latency

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: 50

Options: 0 to 214,748,364 ms

Function: Specifies the maximum latency for a reserved flow packet, limiting the amount of unreserved data that the link scheduler can transmit. When the data transmit ring reaches a size where the time to transmit the data is greater than the value of this parameter, no more unreserved data will be queued.

Instructions: Reduce the value of this parameter to obtain better delay characteristics for reserved flows, but note that overall throughput may decrease. Increase the default value to improve throughput, but note that reserved-flow delays may increase.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.13

Parameter: Largest Bandwidth

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: 0 (no maximum)

Options: 0 or an integer indicating the percentage of bandwidth

Function: Specifies the maximum bandwidth that a single flow can reserve on this line.

Instructions: Set this parameter as required.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.14

Parameter: Largest Buffer

Path: Configuration Manager > XCVR, FDDI, HSSI, MCT1, or COM connector configured for RSVP > Edit Connector window > **Edit Line Resources**

Default: 0 (no maximum)

Options: 0 or an integer specifying the amount of buffer space

Function: Specifies the maximum buffer space that a single flow can reserve on this line.

Instructions: Set this parameter as required.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.15

OSPF Parameters for Multicast Extensions

OSPF Global Parameters

Parameter: Multicast Extensions

Path: Configuration Manager > Protocols > IP > OSPF/MOSPF > Global
Default: 0
Options: 0 (no multicast forwarding is enabled) | 1 (intra-area multicasting only) | 3 (intra-area and inter-area multicasting) | 5 (intra-area and inter-AS multicasting) | 7 (multicasting everywhere)
Function: Enables OSPF multicast extensions and specifies the type of multicasting.
Instructions: Click on Values and set the parameter as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.3.1.19

Parameter: Multicast Timeout Value

Path: Configuration Manager > Protocols > IP > OSPF/MOSPF > Global
Default: 600
Options: An integer
Function: Specifies in seconds a timer value for timing out MOSPF entries in the forwarding table.
Instructions: Use the default setting, 600 seconds, which is equal to 10 minutes.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.3.1.26

Parameter: Multicast Max Queued Pkts

Path: Configuration Manager > Protocols > IP > OSPF/MOSPF > Global
Default: 64
Options: An integer indicating the number of packets
Function: Controls how many multicast packets OSPF can queue on each slot before it finishes calculating multicast trees.
Instructions: If you specify 0, OSPF drops packets before the tree is calculated.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.3.1.27

Parameter: Multicast Dynamic TTL

Path: Configuration Manager > Protocols > IP > OSPF/MOSPF > Global

Default: Disabled

Options: Enabled │ Disabled

Function: Controls whether MOSPF uses a dynamic TTL threshold. Dynamic TTL means that the TTL threshold may be different for each (source, group, downstream) tuple.

Instructions: For maximum forwarding performance, disable this feature.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.3.1.28

Parameter: Multicast Downstream IGMP Relay

Path: Configuration Manager > Protocols > IP > OSPF/MOSPF > Global

Default: Disable

Options: Enable │ Disable

Function: Specifies whether AS external routes are multicast capable. If you enable this feature, the advertising ASBR sets the multicast bit in the ASE LSAs for those routes, so that they can be used for multicast purposes.

Instructions: By default, all external routes are multicast capable. However, if you know that an ASBR's external routes can be used for unicast only, you must set this parameter to Disable on the ASBR.

For example, consider two ASBRs -- ASBR1 and ASBR2 -- each with a BGP connection to an ISP. You know that all multicast traffic should be injected into the MOSPF domain by ASBR2 because ASBR2 has a DVMRP tunnel to the MBone. To prevent ASBR1 from injecting multicast routes into the MOSPF domain, you set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.3.1.30

OSPF Interface Parameters

Parameter:	**Multicast Forwarding**
Path:	Configuration Manager > Protocols > IP > OSPF/MOSPF > Interfaces
Default:	Multicast
Options:	Blocked │ Multicast │ Unicast
Function:	Specifies the way multicast packets should be forwarded on this interface: not forwarded, forwarded as data link multicasts, or forwarded as data link unicasts. Data link multicasting is not meaningful on point-to-point and NBMA interfaces, and setting ospfMulticastForwarding to 0 effectively disables all multicast forwarding.
Instructions:	If you configured MOSPF globally, specify the way that you want IP to forward multicast packets on this interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.3.5.1.30

PIM Parameters

PIM Global Configuration Parameters

Use the following descriptions to set PIM global configuration parameters.

Parameter:	**Enable**
Path:	Configuration Manager > Protocols > IP > PIM > Global
Default:	Enable
Options:	Enable │ Disable
Function:	Enables and disables PIM support on the router. Enabling PIM on an interface automatically enables IGMP.
Instructions:	To disable PIM after you configure it on the router, specify Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.14.1.2

Parameter: Last Hop Threshold

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: Enable

Options: Enable │ Disable

Function: Indicates whether the last-hop router switches from the shared tree to a source-specific, shortest-path tree. The last-hop router sets up a shortest-path tree when the data rate for the group exceeds the configured traffic threshold rate specified using the Last Hop Data Threshold parameter.

Instructions: Set to Enable if you want the last-hop router to switch from a shared tree to a shortest-path tree to the source of that data. Set to Disable to prevent the last-hop router from switching to the shortest-path tree, regardless of the traffic rate specified using the Last Hop Data Threshold parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.9

Parameter: Last Hop Data Threshold

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 2048

Options: 0 to 65,535 (bytes per second)

Function: Specifies the rate, in bytes per second, at which the last-hop router receives data from the source. If the data rate exceeds the threshold configured on the last-hop router, the last-hop router switches to a shortest-path tree.

Instructions: Specify a data rate threshold from 0 through 64 to enable the last-hop router to immediately switch to the shortest-path tree upon receiving the first packet from the source. Otherwise, the data rate is averaged over the threshold sample interval and the switch is made based on this average.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.10

Parameter: **Rendezvous Point (RP) Threshold**

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: Enable

Options: Enable │ Disable

Function: Indicates whether the RP router switches from a shared tree to a source-specific, shortest-path tree. The RP establishes a shortest-path tree when the data rate exceeds the configured threshold value specified using the RP Data Threshold parameter.

Instructions: Set to Enable if you want the RP router to switch from a shared tree to a shortest-path tree to the source of that data. Set to Disable to prevent the RP router from switching to the shortest-path tree, regardless of the data rate specified using the RP Data Threshold parameter

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.11

Parameter: **RP Data Threshold**

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 1024

Options: 0 to 65,535 (bytes per second)

Function: Specifies the rate, in bytes per second, at which the RP router receives data from the source. If the data rate exceeds the RP data rate threshold, the RP router switches to a shortest-path tree between the source and the RP router.

Instructions: Specify a data rate threshold from 0 through 64 to enable the RP router to immediately switch from the shared tree to the shortest-path tree upon receiving the first packet from the source. Otherwise, the date rate is averaged over the threshold sample interval and the switch is made based on this average.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.12

Parameter: Threshold Sample Interval

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 16

Options: 16 to 300 (seconds)

Function: Specifies the interval, in seconds, at which the PIM router calculates the average rate of the current data flow to determine the data threshold. This sampling time is a multiple of 16 seconds. If the value specified is not a multiple of 16, the PIM router uses the multiple of 16 lower than this value.

Use this parameter to reduce the CPU load from calculation during data forwarding.

Instructions: Determine a threshold sample interval and enter this value. The highest value, 300 seconds, is equal to 5 minutes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.13

Parameter: Default Join/Prune Interval

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 60

Options: 5 to 18,724 (seconds)

Function: Specifies the default interval, in seconds, at which each PIM interface configured on the local router sends join/prune messages to its upstream neighbor.

Instructions: Specify an interval value that all interfaces configured on the local router can use as the default join/prune interval. The highest value, 18,724 seconds, is equal to 5 hours, 12 minutes, and 4 seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.8

Parameter: Generate Neighbor Hello ID

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: Enable

Options: Enable │ Disable

Function: Specifies whether the Hello message sent by the PIM router to its neighbors contains a generation identifier. A generation identifier is a randomly assigned number that remains static as long as the router is active. The PIM router uses the generation identifier to quickly learn whether a neighbor rebooted within the holdtime specified in its previous Hello message.

When a neighbor reboots, it is assigned a new generation identifier and immediately sends a Hello message that contains the new generation ID. The generation ID triggers a DR on the LAN to send the most recent RP set information to the neighbor that just rebooted.

Instructions: Set to Enable to allow the PIM router to send Hello packets that contain a generation identifier to its neighbors. Set to Disable to prevent the PIM router from sending Hello packets that contain a generation identifier to its neighbors.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.15

Parameter: Candidate BSR

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: Disable

Options: Enable │ Disable

Function: Specifies whether to configure a PIM router as a C-BSR.

PIM elects the C-BSR with the highest configured priority as the primary BSR for the domain. If two C-BSRs have equal priority, then PIM elects the C-BSR with the higher IP address as the BSR for the domain.

Instructions: Set to Enable to configure a PIM router as a C-BSR. Set to Disable to prevent a PIM router from being elected as the primary BSR for the domain.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.20

Parameter: Candidate BSR IP Address

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 0.0.0.0

Options: Any valid IP address or a circuitless IP address

Function: Specifies the IP address or circuitless IP address for a C-BSR. PIM uses the C-BSR to distribute the RP set information to all routers in the PIM domain.

Instructions: Specify an IP address or circuitless IP address for each C-BSR in a PIM domain in dotted-decimal notation.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.21

Parameter: Candidate BSR Priority

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 0

Options: 0 to 255

Function: Specifies the priority level assigned to the C-BSR. The higher the number, the higher the priority. PIM elects the C-BSR with the highest priority as the primary BSR for the PIM domain. If two C-BSRs have equal priority, then PIM elects the C-BSR with the higher IP address as the BSR for the domain.

Instructions: Determine a priority level for the C-BSR and enter this value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.22

Parameter: Candidate BSR Interval

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 60

Options: 5 to 32,757 (seconds)

Function: Specifies the interval, in seconds, at which the elected BSR multicasts periodic bootstrap messages (RP set) on all PIM interfaces.

Instructions: Specify a value from 5 through 32,757 that determines how frequently the elected BSR sends periodic RP-set messages on all PIM interfaces. The highest possible value, 32,757 seconds, is equal to 9 hours, 5 minutes, and 57 seconds. You must specify the same interval for each C-BSR in the PIM domain.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.23

Parameter: Candidate BSR Hash Mask Length

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 30

Options: 4 to 32

Function: Specifies the length of the hash mask for the elected BSR. The hash function is used by all routers within a PIM domain to map a group to one of the C-RPs in the RP set. For a particular group, G, the hash function uses only those C-RPs whose group prefix covers G. The hash function takes as input the group address and the addresses of the C-RPs, and gives as output one RP address to be used.

The hash mask, which is included in the bootstrap message, allows a small number of consecutive groups (for example, 4) to map to the same RP. For example, hierarchically encoded data can be sent on consecutive group addresses to obtain the same delay and fate-sharing characteristics.

Instructions: Determine the length of the hash mask and specify a value from 4 through 32.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.24

Parameter: Candidate RP

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: Disable

Options: Enable │ Disable

Function: Specifies whether to configure a PIM router as a C-RP router. C-RP routers periodically send unicast C-RP advertisement messages to the BSR of that domain. The interval for sending C-RP messages is specified using the Candidate RP Advertise Interval parameter.

PIM elects the primary RP based on priority first, then on the highest hash value. If the priority level and hash value are the same, PIM elects the C-RP with the highest IP address as the RP.

Instructions: Set to Enable to configure the PIM router as a C-RP. Set to Disable if you do not want to configure the PIM router as a C-RP.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.25

Parameter:	**Candidate RP IP Address**
Path:	Configuration Manager > Protocols > IP > PIM > Global
Default:	0.0.0.0
Options:	Any valid IP address or a circuitless IP address
Function:	Specifies the IP address or circuitless IP address for the C-RP. PIM uses this IP address to map the configured group or group ranges to the RP. First-hop routers use the RP address to send register messages on behalf of a source sending a packet to the group. Last-hop routers use the RP address to send join/prune messages to the RP to inform it about group membership.
Instructions:	Specify an IP address or circuitless IP address for the C-RP in dotted-decimal notation.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.14.1.26

Parameter:	**Candidate RP Priority**
Path:	Configuration Manager > Protocols > IP > PIM > Global
Default:	0
Options:	0 to 255
Function:	Specifies the priority level for the C-RP. PIM elects the RP based on priority first, then on the highest hash value. If the priority level and hash value are the same, PIM elects the C-RP with the highest IP address as the RP; the other C-RPs serve as backups in case the RP fails.
Instructions:	Determine the priority level for the C-RP and enter a value. You must specify a priority level for each C-RP in the PIM domain.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.14.1.23

Parameter: Candidate RP Group/Mask

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: Null (all groups)

Options: List of multicast group addresses and masks

Function: Specifies the list of IP multicast group addresses and masks to which the C-RP maps, for example:

IP Address	Mask
224.1.1.0	255.255.255.0
225.1.0.0	255.255.0.0
225.1.1.16	255.255.255.240

Instructions: Click on Values and specify the list of multicast group addresses and masks in dotted-decimal notation.

MIB Object ID: Not applicable

Parameter: Candidate RP Advertise Interval

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 60

Options: 5 to 26,214 (seconds)

Function: Specifies how often the C-RP router sends periodic unicast C-RP advertise messages to the BSR for this domain.

Instructions: Either accept the default value of 60 seconds or set the C-RP advertise interval to a value within the allowable range. The highest allowable value, 26,214 seconds, is equal to 7 hours, 16 minutes, and 54 seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.29

Parameter:	**Candidate RP Register Cache Timeout**
Path:	Configuration Manager > Protocols > IP > PIM > Global
Default:	210
Options:	5 to 65,535 (seconds)
Function:	Specifies a timeout value, in seconds, for all cache entries whose inbound interface is created from PIM register packets received on the RP router. If the RP router does not receive the PIM register packet within the specified period of time, it deletes the forwarding cache entry associated with this interface.
Instructions:	Determine the timeout period that you require and specify a value. The highest allowable value, 65,535 seconds, is equal to 18 hours, 12 minutes, and 15 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.14.1.31

Parameter:	**Register Suppression Timeout**
Path:	Configuration Manager > Protocols > IP > PIM > Global
Default:	60
Options:	5 to 65,535 (seconds)
Function:	Specifies the time period, in seconds, during which the first-hop router (DR) disables the sending of register messages to the RP after receiving a register-stop message from the RP. The RP sends a register-stop message when it receives unencapsulated data packets from the DR and there are no downstream routers (receivers) to forward these packets to.
Instructions:	Determine the timer interval that you require and specify a value. The highest allowable value, 65,535 seconds, is equal to 18 hours, 12 minutes, and 15 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.14.1.33

Parameter: **Probe Time**

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 5

Options: 0 to 65,535 (seconds)

Function: Specifies the interval, in seconds, between the time that the first-hop router sends a probe packet (null register packet with no user data) to the RP router and the expiration of the register suppression timer, unless it is restarted by receiving a register-stop message.

Instructions: Specify a value of 0 to prevent the first-hop router from sending a probe packet to the RP. If you specify a value greater than 0, it must be less than the register suppression timeout value, otherwise it does not take effect. The highest allowable value, 65,535 seconds, is equal to 18 hours, 12 minutes, and 15 seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.34

Parameter: **Cisco Compatible**

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: Disable

Options: Enable | Disable

Function: Allows Bay Networks routers to interoperate with Cisco routers running a nonstandard PIM implementation.

Instructions: By default, this parameter is disabled to ensure that Bay Networks routers comply with the standard PIM specification defined in RFC 2362. To allow Bay Network routers to interoperate with Cisco routers configured with a nonstandard implementation of PIM, set this parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.35

Parameter: **Info/Warnings**

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 0

Options: 0 | PIM modules for which you want to log info/warning messages

Function: Enables or disables the logging of PIM informational and warning messages on the PIM router.

Instructions: To disable logging of PIM informational and warning messages, accept the default value, 0. To enable logging of these messages, click on Values and select the PIM modules for which you want to log info/warning messages. The modules that you select are represented as bits values in the parameter field, as follows:

0x00000001 -- Bootstrap procedure
0x00000002 -- Hello procedure
0x00000004 -- Join/prune send procedure
0x00000008 -- Registration procedure
0x00000010 -- Maintaining PIM route table
0x00000020 -- Assert procedure
0x00000040 -- Data forwarding/tree switching
0x00000080 -- PIM main gate processing
0x00000100 -- PIM Cct gate general processing
0x00000200 -- PIM route change processing
0x00000400 -- PIM (*,G) processing
0x00000800 -- PIM pte/oif timers
0x00002000 -- PIM-PIM messages
0x00004000 -- PIM protocol messages/first data
0x00008000 -- Join/prune received
0x00010000 -- PIM utilities including timers

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.4

Parameter: Debug

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 0

Options: 0 | PIM modules for which you want to log PIM debug messages

Function: Enables or disables the logging of PIM debugging messages on the PIM router.

Instructions: To disable logging of PIM debug messages, accept the default value, 0. To enable logging of these messages, click on Values and select the PIM modules for which you want to log debug messages. The modules that you select are represented as bits values in the parameter field, as follows:

0x00000001 -- Bootstrap procedure
0x00000002 -- Hello procedure
0x00000004 -- Join/prune send procedure
0x00000008 -- Registration procedure
0x00000010 -- Maintaining PIM route table
0x00000020 -- Assert procedure
0x00000040 -- Data forwarding/tree switching
0x00000080 -- PIM main gate processing
0x00000100 -- PIM Cct gate general processing
0x00000200 -- PIM route change processing
0x00000400 -- PIM (*,G) processing
0x00000800 -- PIM pte/oif timers
0x00001000 -- PIM-MTM signals/messages
0x00002000 -- PIM-PIM messages
0x00004000 -- PIM protocol messages/first data
0x00008000 -- Join/prune received
0x00010000 -- PIM utilities including timers
0x00020000 -- PIM debug option for ip pim_fwd

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.5

Parameter: Trace

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 0

Options: 0 | PIM modules for which you want to log PIM trace messages

Function: Enables or disables the logging of PIM trace messages on the PIM router.

Instructions: To disable logging of PIM trace messages, accept the default value, 0. To enable logging of these messages, click on Values and select the PIM modules for which you want to log trace messages. The modules that you select are represented as bits values in the parameter field, as follows:

0x00000001 -- Bootstrap procedure
0x00000002 -- Hello procedure
0x00000004 -- Join/prune send procedure
0x00000008 -- Registration procedure
0x00000010 -- Maintaining PIM route table
0x00000020 -- Assert procedure
0x00000040 -- Data forwarding/tree switching
0x00000080 -- PIM main gate processing
0x00000100 -- PIM Cct gate general processing
0x00000200 -- PIM route change processing
0x00000400 -- PIM (*,G) processing
0x00000800 -- PIM pte/oif timers
0x00002000 -- PIM-PIM messages
0x00004000 -- PIM protocol messages/first data
0x00008000 -- Join/prune received
0x00010000 -- PIM utilities including timers

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.6

PIM Interface Parameters

Use the following descriptions to set PIM interface parameters.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > PIM > Interface

Default: Enable

Options: Enable | Disable

Function: Enables or disables PIM on this interface.

Instructions: After you configure PIM on an interface, PIM is enabled by default. To disable PIM on this interface without deleting it, enter Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.2.1.2

Parameter: Hello Interval

Path: Configuration Manager > Protocols > IP > PIM > Interface

Default: 30

Options: 1 to 2,147,483,647 (seconds)

Function: Specifies how often, in seconds, the local PIM router sends Hello messages on this PIM interface. PIM routers periodically send Hello messages so that PIM neighbors can discover each other. Hello messages are multicast using address 224.0.0.13 (all PIM routers group) and are sent on all communication links.

Instructions: Either accept the default value of 30 seconds or set the Hello interval to another value. Bay Networks recommends a higher number for slower-speed serial lines.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.2.1.8

Parameter: Cache Time Out

Path: Configuration Manager > Protocols > IP > PIM > Interface

Default: 210

Options: 5 to 2,147,483,647 (seconds)

Function: Specifies the amount of time, in seconds, that data entries remain in the PIM cache before timing out.

Instructions: Specify a value, in seconds, that represents the duration of time that the data entry remains in the PIM cache before being deleted.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.2.1.9

Parameter: Use Global Join/Prune Interval

Path: Configuration Manager > Protocols > IP > PIM > Interface

Default: Enable

Options: Enable | Disable

Function: Specifies whether or not the PIM router sends periodic join/prune messages on this interface based on the interval specified using the global Default Join/Prune Interval parameter.

Instructions: Set to Enable if you want the PIM router to use the join/prune interval specified using the global Default Join/Prune Interval parameter. Set to Disable if you want the PIM router to use the join/prune interval specified using the Join/Prune Interval parameter on this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.2.1.10

Parameter: Join/Prune Interval

Path: Configuration Manager > Protocols > IP > PIM > Interface

Default: 60

Options: 1 to 65,535 seconds

Function: Specifies the time period, in seconds, at which the PIM router sends periodic join/prune messages on this PIM interface. This interval takes effect only if you disabled the Use Global Join/Prune Interval parameter.

Instructions: Determine the join/prune interval that you require and specify a value from 1 through 65,535 seconds (18 hours, 12 minutes, and 15 seconds).

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.2.1.11

Parameter: Downstream IGMP Relay

Path: Configuration Manager > Protocols > IP > PIM > Interface

Default: Disable

Options: Enable │ Disable

Function: Indicates whether you want to enable or disable support for IGMP Relay on a downstream router.

Instructions: Set to Enable to allow the PIM router to receive multicast data from a downstream router configured with IGMP Relay, encapsulate the data within a register packet, and send the packet to the elected RP in the PIM domain.

If you enable this parameter on a PIM interface, you must configure all other PIM routers on the same physical link to enable this parameter on the same PIM interface.

If you set this parameter to Disable, the PIM router drops multicast packets forwarded from the IGMP Relay router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.2.1.12

Parameter:	**Local DR Priority**
Path:	Configuration Manager > Protocols > IP > PIM > Interface
Default:	1
Options:	0 to 65,535
Function:	Specifies the priority level for a DR on the LAN, regardless of the IP address of the other PIM routers on the LAN. The higher the number, the higher the priority. Each PIM router on which you configured a DR election priority sends to its PIM neighbors a Hello message that contains its priority level. The PIM router with the highest priority level is elected the DR for the LAN. Local routers not configured with a DR election priority elect a DR based on the highest IP address. A value of 0 disables this feature on the LAN.
Instructions:	Enter a priority value from 1 through 65,535. To disable the DR election priority option on the LAN, enter a priority value of 0.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.14.2.1.13

RSVP Parameters

RSVP Global Parameters

Parameter:	**Enable**
Path:	Configuration Manager > Protocols > IP > RSVP > Global
Default:	Enable
Options:	Enable | Disable
Function:	Specifies the state of global RSVP.
Instructions:	Disable and reenable global RSVP as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.16.1.1.1.2

Parameter: Soloist Slots

Path: Configuration Manager > Protocols > IP > RSVP > Global
Default: All slots
Options: Slots 1 to 14
Function: Specifies the slot or slots on which RSVP is eligible to run.
Instructions: Select a slot or slots for global RSVP.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.1.1.4

Parameter: Info Log Filter

Path: Configuration Manager > Protocols > IP > RSVP > Global
Default: 0
Options: 0 | RSVP modules for which you want to log informational messages
Function: Enables or disables logging of informational messages for the specified RSVP modules.
Instructions: To disable logging of RSVP informational messages, accept the default value, 0. To enable logging, click on Values and select the RSVP modules for which you want to log informational messages.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.1.1.5

Parameter: Debug Log Filter

Path: Configuration Manager > Protocols > IP > RSVP > Global
Default: 0
Options: 0 | RSVP modules for which you want to log debug messages
Function: Enables or disables logging of debug messages for the specified RSVP modules.
Instructions: To disable logging of RSVP debug messages, accept the default value, 0. To enable logging, click on Values and select the RSVP modules for which you want to log debug messages.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.1.1.6

Parameter: **Trace Log Filter**

Path: Configuration Manager > Protocols > IP > RSVP > Global

Default: 0

Options: 0 | RSVP modules for which you want to log trace messages

Function: Enables or disables logging of trace messages for the specified RSVP modules.

Instructions: To disable logging of RSVP trace messages, accept the default value, 0. To enable logging, click on Values and select the RSVP modules for which you want to log trace messages.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.1.1.7

RSVP Interface Parameters

Parameter: **Enable**

Path: Configuration Manager > Protocols > IP > RSVP > Circuit

Default: Enable

Options: Enable | Disable

Function: Sets the state of RSVP on this interface.

Instructions: Disable and reenable RSVP on the interface as required.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.1.6.1.2

Parameter: **Refresh Blockade Multiple**

Path: Configuration Manager > Protocols > IP > RSVP > Circuit

Default: 4

Options: 1 to 65,536

Function: Specifies the number of refresh intervals that RSVP will stay alive in the blockade state.

Instructions: Specify the number of refresh intervals for the blockade state.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.1.6.1.8

Parameter: Refresh Multiple

Path:	Configuration Manager > Protocols > IP > RSVP > Circuit
Default:	3
Options:	1 to 65,536
Function:	Specifies the number of refresh intervals that must elapse before a PATH or RESV message that is not refreshed will time out.
Instructions:	Specify the number of refresh intervals for a PATH or RESV message.
MIB Object ID:	1.3.6.1.4.1.18.3.5.16.1.1.6.1.9

Parameter: RSVP TTL

Path:	Configuration Manager > Protocols > IP > RSVP > Circuit
Default:	0 (no TTL override)
Options:	0 to 255
Function:	Specifies a TTL value used on this interface for messages that this node originates. If set to a value other than 0, the node determines the TTL via other means. This overrides the IP TTL value.
Instructions:	Set the TTL to 0 if you want the node to use the IP TTL value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.16.1.1.6.1.10

Parameter: Refresh Interval

Path:	Configuration Manager > Protocols > IP > RSVP > Circuit
Default:	3000
Options:	An integer indicating the refresh interval in hundredths of a second
Function:	Specifies the minimum period between refresh transmissions of a given PATH or RESV message on an interface.
Instructions:	Specify the interval in hundredths of a second. The default, 3000 hundredths of a second, is equal to 30 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.16.1.1.6.1.11

Parameter:	**Route Delay**
Path:	Configuration Manager > Protocols > IP > RSVP > Circuit
Default:	200
Options:	An integer indicating the route delay in hundredths of a second
Function:	Specifies the approximate period from the time that a route is changed to the time that a resulting message appears on the interface.
Instructions:	Specify the delay period in hundredths of a second. The default, 200 hundredths of a second, is equal to 2 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.16.1.1.6.1.12

Parameter:	**Udp Required**
Path:	Configuration Manager > Protocols > IP > RSVP > Circuit
Default:	False
Options:	True | False
Function:	Specifies whether or not UDP encapsulation is used on this interface.
Instructions:	Select True if manual configuration forces RSVP to use UDP encapsulation on the interface. Select False to disable UDP encapsulation. If you select False, RSVP uses UDP encapsulation only if it determines that a neighbor on this interface also uses UDP encapsulation.
MIB Object ID:	1.3.6.1.4.1.18.3.5.16.1.1.6.1.13

Multicast Policy Parameters

Topic	Page
DVMRP Unicast Accept Policy Parameters	A-59
DVMRP Accept Policy Parameters	A-64
DVMRP Announce Policy Parameters	A-69
MOSPF Accept DVMRP Route Policy Parameters	A-73
IGMP Group Policy Parameters	A-76
IGMP Static Forwarding Policy Parameters	A-80
IGMP Boundary Group Parameters	A-84

DVMRP Unicast Accept Policy Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Unicast Accept Policies
Default: Enabled
Options: Enabled │ Disabled
Function: Enables and disables this policy.
Instructions: Set this parameter as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.17.1.2

Parameter: Name

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Unicast Accept Policies
Default: None
Options: A character string
Function: Supplies a name for this policy.
Instructions: Enter a unique name to identify this policy.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.17.1.4

Parameter: Incoming Networks

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Unicast Accept Policies

Default: Null

Options: A list of IP addresses

Function: Specifies the network or networks that match this policy.

Instructions: Enter an IP address in the following form:

First octet: exact (1) or range (2)
Next 4 octets: network number
Next 4 octets: network mask

An entry with an exact tag means: match the specific network advertisement (number and mask). An entry with a range tag means: match any network number that falls in the range indicated by the number and mask.

To match any address, accept the default, null.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.17.1.5

Parameter: Action

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Unicast Accept Policies

Default: Accept

Options: Accept | Ignore

Function: Specifies the action that DVMRP performs on a route that matches this policy.

Instructions: Select Accept to import the matching route from the IP unicast routing table to the DVMRP routing table. If you do not want to import the matching route, select Ignore.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.17.1.6

Parameter: Route Preference

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Unicast Accept Policies

Default: 0

Options: 0 to 16

Function: Specifies a value that DVMRP uses to compare the route for injection to an existing route in the DVMRP routing table. This parameter has meaning only if the action is Accept.

Instructions: If the injected unicast route is preferred, set the preference to a higher value than the preference value of the existing route. A route learned from a DVMRP network always has a preference of 1.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.17.1.7

Parameter: Rule Precedence

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Unicast Accept Policies

Default: 0

Options: 0 to 2147483647

Function: Specifies a metric that DVMRP uses to compare this policy to other policies that match the route. DVMRP uses the precedence value to choose among multiple matches.

Instructions: In ranking policies according to precedence, keep in mind that the route with the highest value is the preferred route. In case of a tie, the route with the larger index number wins.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.17.1.8

Parameter:	**Inject Aggregate**
Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Unicast Accept Policies
Default:	Null
Options:	An IP address and mask
Function:	Specifies an IP network that DVMRP injects into the DVMRP routing table in place of the advertised networks. This parameter has meaning only if the action is Accept.
Instructions:	Enter an IP address and mask. To inject the learned network, use the default, null. Use this parameter to inject an aggregate address for a range of learned networks. This allows insertion of an aggregate or default network along with the actual network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.17.1.9

Parameter:	**Received on Interfaces**
Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Unicast Accept Policies
Default:	Null
Options:	A list of IP interfaces
Function:	Specifies a list of inbound interfaces. This policy applies to advertisements that arrive on the interfaces on this list.
Instructions:	To apply the policy to advertisements that arrive on any interface, use the default, null.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.17.1.10

Parameter: Route Type

Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Unicast Accept Policies
Default:	Best route
Options:	Best route | OSPF | Both
Function:	Specifies the type of route that DVMRP selects from the IP unicast routing table.
Instructions:	Set this parameter as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.17.1.11

Parameter: Metric

Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Unicast Accept Policies
Default:	1
Options:	1 to 31
Function:	Specifies the cost of the route that DVMRP injects into the DVMRP routing table.
Instructions:	Set this parameter as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.17.1.12

DVMRP Accept Policy Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Accept Policies
Default: Enabled
Options: Enabled │ Disabled
Function: Enables or disables this accept policy.
Instructions: Set this parameter as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.15.1.2

Parameter: Name

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Accept Policies
Default: None
Options: A character string
Function: Specifies the name of this policy.
Instructions: Enter a unique name to identify the policy.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.15.1.4

Parameter: Incoming Networks

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Accept Policies

Default: Null

Options: A list of IP addresses

Function: Specifies networks that match this rule.

Instructions: To specify a network, enter the address in the following format:

First octet: exact (1) or range (2)
Next 4 octets: network number
Next 4 octets: network mask

Exact means: match only the specific network advertisement (number and mask). Range means: match any network number that falls in the range indicated by the number and mask.

An exact encoding of 0.0.0.0/0.0.0.0 means: match the default route. A range encoding of 0.0.0.0/0.0.0.0 means: match any route.

A null string also means: match any route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.15.1.5

Parameter: Action

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Accept Policies

Default: Accept

Options: Accept | Ignore

Function: Specifies the action that DVMRP performs on a route that matches this policy.

Instructions: Select Accept to consider the route for inclusion in the routing table. Select Ignore if you do not want to consider the route for inclusion.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.15.1.6

Parameter: Rule Precedence

Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Accept Policies
Default:	0
Options:	0 to 2147483647
Function:	Supplies a metric that DVMRP uses to compare this policy to other policies that a given route may match. DVMRP chooses a policy with higher precedence over one with a smaller value. In the case of a tie, DVMRP uses the policy with the larger index.
Instructions:	Set this parameter as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.15.1.8

Parameter: Inject Aggregate

Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Accept Policies
Default:	Null
Options:	An IP address and mask
Function:	Specifies an IP network that DVMRP injects into the DVMRP routing table in place of the advertised networks. This parameter has meaning only if the action is Accept. Use this parameter to inject an aggregate address for a range of learned networks. This allows insertion of an aggregate or default network along with the actual network.
Instructions:	Enter an IP address and mask. To inject the learned network, use the default, null.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.15.1.9

Parameter: Incoming Gateways

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Accept Policies

Default: Null

Options: A list of IP addresses

Function: Specifies the addresses of one or more routers that can send DVMRP updates to this router. If you configure a list, this policy applies to DVMRP advertisements from the routers in the list.

Instructions: To apply this policy to any router, use the default, null.

If non-null, the octet string contains one or more 4-octet IP addresses.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.15.1.10

Parameter: Received on Interfaces

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Accept Policies

Default: Null

Options: A list of IP addresses

Function: Specifies a list of inbound interfaces. This policy applies to advertisements that arrive on the interfaces on this list.

Instructions: To create a policy that applies to advertisements that arrive on any interface, accept the default, null.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.15.1.11

Parameter:	**Received on Tunnels**
Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Accept Policies
Default:	Null
Options:	A list of tunnel specifications
Function:	Specifies one or more DVMRP tunnels. If a tunnel interface appears in this list, this policy applies to DVMRP advertisements sent via that tunnel.
Instructions:	For each tunnel, enter an 8-octet specification. The first four octets are the local IP address; the second four octets are the remote IP address. If you want the policy to apply to any tunnel, use the default, null. If you want the policy to apply to no tunnels, enter a tunnel specification consisting of all Fs.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.15.1.13

Parameter:	**Metric**
Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Accept Policies
Default:	1
Options:	1 to 31
Function:	Specifies the cost of the route that DVMRP injects into the DVMRP routing table.
Instructions:	Set this parameter as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.15.1.14

DVMRP Announce Policy Parameters

Use the following descriptions to set DVMRP announce policies.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies
Default: Enable
Options: Enable | Disable
Function: Enables or disables this policy.
Instructions: Set this parameter as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.2

Parameter: Name

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies
Default: None
Options: A character string
Function: Specifies the name of this policy.
Instructions: Enter a unique name to identify this policy.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.4

Parameter: Incoming Networks

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies
Default: An empty list
Options: A list of network identifiers. Each identifier consists of a network number, a mask, and a flag to indicate whether the ID refers to a specific network or a range of networks.
Function: Specifies which networks match this policy.
Instructions: Enter an empty list to match any route.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.5

Parameter: Action

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies

Default: Announce

Options: Announce | Ignore

Function: Specifies whether to advertise a route that matches this policy.

Instructions: To advertise the route, specify Announce. To drop the route, specify Ignore.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.6

Parameter: Rule Precedence

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies

Default: 0

Options: An integer

Function: Specifies a value to be used to compare this policy with other policies that a route may match. A policy with a higher value takes precedence over a policy with a lower value. In case of a tie, the protocol uses an internal index value assigned to the policy by IP software. The position of the policy in the list indicates the index value from lowest to highest.

Instructions: Use this parameter to assign precedence to policies that match the same route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.7

Parameter: Advertise Aggregate

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies

Default: Null

Options: IP address and mask

Function: Advertises a network that differs from the actual network in the routing table.

Instructions: This octet string should only be non-null if the action is Announce, and if you want to advertise a network that differs from the actual network in the routing table. For example, if a number of networks in a certain range are in the table, an aggregate could be advertised instead of the individual networks.

If non-null, the octet string contains one or more 2-tuples of the following form:

First 4 octets: network number
Next 4 octets: network mask

Upon receiving a route that matches this policy, all networks in this list will be advertised. If the list is null, the actual network is advertised.

An encoding of 255.255.255.255/255.255.255.255 means match the actual network. This allows advertisement of an aggregate or default along with the actual network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.10

Parameter: Outgoing Interfaces

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies

Default: An empty list

Options: Leave empty or specify IP addresses.

Function: Specifies a list of DVMRP interfaces. By specifying an interface in this list, the policy applies to DVMRP advertisements sent using that interface.

Instructions: If you want this policy to apply to any outbound DVMRP interface, do not specify a value for this parameter. If you want this policy to apply to specific outbound DVMRP interfaces, specify the interface IP addresses.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.25

Parameter:	**Outgoing Tunnels**
Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies
Default:	An empty list
Options:	Leave empty or specify one or more 8-octet tunnel specifications.
Function:	Specifies a list of DVMRP tunnels. If a tunnel interface appears in this list, the filter applies to DVMRP advertisements sent via that tunnel. Each tunnel takes eight octets, the first four of which are for the local IP address and the last four for the remote IP address.
Instructions:	If you want this filter to apply to any DVMRP tunnel, do not specify any value for this parameter. If you want this filter to apply to specific DVMRP tunnels, specify the IP addresses in 8-octet strings. Entering all Fs for the first IP address turns off this filter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.16.1.23

Parameter:	**Metric**
Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies
Default:	0
Options:	0 to 31
Function:	Specifies a metric for routes specified in the network identification list.
Instructions:	To advertise the routes with the metric values in the routing table, accept the default, 0. To specify a different metric value, set this parameter as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.16.1.24

MOSPF Accept DVMRP Route Policy Parameters

Use the following descriptions to set MOSPF accept DVMRP route policies.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > Policy Filters > MOSPF > Accept DVMRP Route Policies
Default: Enable
Options: Enable | Disable
Function: Enables or disables this policy.
Instructions: Set this parameter as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.14.1.2

Parameter: Name

Path: Configuration Manager > Protocols > IP > Policy Filters > MOSPF > Accept DVMRP Route Policies
Default: None
Options: Any alphanumeric character string
Function: Identifies this policy.
Instructions: Enter a unique name for the policy.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.14.1.4

Parameter: Action

Path: Configuration Manager > Protocols > IP > Policy Filters > MOSPF > Accept DVMRP Route Policies
Default: Accept
Options: Accept | Ignore
Function: Specifies whether the DVMRP route should be used by MOSPF.
Instructions: To advertise the route, specify Accept. To drop the route, specify Ignore.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.14.1.6

Parameter: Rule Precedence

Path:	Configuration Manager > Protocols > IP > Policy Filters > MOSPF > Accept DVMRP Route Policies
Default:	0
Options:	An integer
Function:	Specifies a metric value to be used to compare this policy with other policies that a route may match. A policy with a higher metric takes precedence over a policy with a lower metric. In case of a tie, the protocol uses an internal index value assigned to the policy by IP software. The position of the policy in the list indicates the index value from lowest to highest.
Instructions:	Use this parameter to assign precedence to policies that match the same route.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.14.1.7

Parameter: DVMRP Networks

Path:	Configuration Manager > Protocols > IP > Policy Filters > MOSPF > Accept DVMRP Route Policies
Default:	An empty list
Options:	A list of network identifiers
Function:	Specifies which networks match this policy. Each identifier consists of a network number, a mask, and a flag to indicate whether the ID refers to a specific network or a range of networks.
Instructions:	Accept the default to match any route, or specify the networks that match this policy.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.14.1.5

Parameter:	**Inject List**
Path:	Configuration Manager > Protocols > IP > Policy Filters > MOSPF > Accept DVMRP Route Policies
Default:	An empty list
Options:	See below.
Function:	Advertises networks that differ from the actual network in the routing table.
Instructions:	This octet string should only be non-null if the action is Accept, and if you want to advertise networks that differ from the actual network in the routing table. For example, if a number of networks in a certain range are in the table, an aggregate could be advertised instead of the individual networks. If non-null, the octet string contains one or more 2-tuples in the following form: First 4 octets: network number Next 4 octets: network mask Upon receiving a route that matches this filter, the router advertises all networks in this list. If the list is null, the router advertises the actual network. An encoding of 255.255.255.255/255.255.255.255 means match the actual network. This allows advertisement of an aggregate or default along with the actual network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.14.1.10

IGMP Group Policy Parameters

Use the following descriptions to set IGMP group policies.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Group Policies
Default: Enable
Options: Enable | Disable
Function: Enables or disables this policy.
Instructions: Set this parameter as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.11.1.2

Parameter: Name

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Group Policies
Default: None
Options: A character string
Function: Specifies the name for this policy.
Instructions: Enter a unique name to identify this policy.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.11.1.4

Parameter: Sources

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Group Policies

Default: An empty list

Options: Leave empty or specify one or more sources.

Function: Identifies which sources will match this policy.

Instructions: If you want this filter to match any source, do not specify a value for this parameter.

To specify an exact source address or range of source addresses, enter one or more octet groupings in the following form:

First octet: exact (1) or range (2)

Next 4 octets: source address

Next 4 octets: source mask

Exact means: match only the specific source (number and mask). Range means: match any prefix that falls in the range indicated by the source and mask.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.11.1.5

Parameter: Action

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Group Policies

Default: Ignore

Options: Accept │ Ignore

Function: Specifies whether to accept or ignore the group join.

Instructions: Specify Accept to accept the group join, or Ignore to ignore the group join.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.11.1.6

Parameter: Rule Precedence

Path:	Configuration Manager > Protocols > IP > Policy Filters > IGMP > Group Policies
Default:	0
Options:	A metric value
Function:	Specifies a metric value to be used to compare this policy with other policies that a route may match. A policy with a higher metric takes precedence over a policy with a lower metric. In case of a tie, the protocol uses an internal index value assigned to the policy by IP software. The position of the policy in the list indicates the index value from lowest to highest.
Instructions:	Use this parameter to assign precedence to policies that match the same route.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.11.1.8

Parameter: Groups

Path:	Configuration Manager > Protocols > IP > Policy Filters > IGMP > Group Policies
Default:	An empty list
Options:	Leave empty or specify one or more groups.
Function:	Identifies which groups match this policy.
Instructions:	If you want this filter to match any group, do not specify a value for this parameter. To match specific groups, enter group number and group mask combinations as follows: First 4 octets: group number Next 4 octets: group mask
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.11.1.10

Parameter: Receivers' Circuits

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Group Policies

Default: An empty list

Options: Leave empty or specify one or more 2-octet circuit numbers.

Function: Identifies which circuits match this policy.

Instructions: If you want this filter to match any circuit, do not specify a value for this parameter.

If you want this filter to apply to specific circuits, enter the circuit numbers in 2-octet strings.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.11.1.11

Parameter: Receivers

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Group Policies

Default: An empty list

Options: Leave empty or specify one or more receiver address and receiver mask octet combinations.

Function: Identifies which receivers match this policy.

Instructions: If you want this filter to match any receiver, do not specify a value for this parameter.

To match specific receivers, enter the receiver address and receiver mask combinations as follows:

First 4 octets: receiver address
Next 4 octets: receiver mask

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.11.1.12

IGMP Static Forwarding Policy Parameters

Use the following descriptions to set IGMP static forwarding policies.

Parameter: Enable

Path:	Configuration Manager > Protocols > IP > Policy Filters > IGMP > Static Forwarding Entries
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables this policy.
Instructions:	Set this parameter as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.20.1.2

Parameter: Name

Path:	Configuration Manager > Protocols > IP > Policy Filters > IGMP > Static Forwarding Entries
Default:	None
Options:	A character string
Function:	Specifies the name of this policy.
Instructions:	Enter a unique name to identify the policy.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.20.1.4

Parameter: Groups

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Static Forwarding Entries

Default: An empty list

Options: Leave empty or specify one or more groups.

Function: Identifies which groups match this policy.

Instructions: If you want this filter to match any group, do not specify a value for this parameter.

To match specific groups, enter group number and group mask combinations as follows:

First 4 octets: group number
Next 4 octets: group mask

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.20.1.5

Parameter: Rule Precedence

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Static Forwarding Entries

Default: 0

Options: An integer

Function: Specifies a metric value to compare this policy with other policies that a route may match. A policy with a higher value takes precedence over a policy with a lower value. In case of a tie, the protocol uses an internal index value assigned to the policy by IP software. The position of the policy in the list indicates the index value from lowest to highest.

Instructions: Use this parameter to assign precedence to policies that match the same route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.20.1.8

Parameter: Sources

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Static Forwarding Entries

Default: An empty list

Options: Leave empty or specify one or more sources.

Function: Identifies which sources will match this policy.

Instructions: If you want this filter to match any source, do not specify a value for this parameter.

To specify an exact source address or range of source addresses, enter one or more octet groupings in the following form:

First octet: exact (1) or range (2)

Next 4 octets: source address

Next 4 octets: source mask

Exact means: match only the specific source (number and mask). Range means: match any prefix that falls in the range indicated by the source and mask.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.20.1.10

Parameter: In Circuits

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Static Forwarding Entries

Default: An empty list

Options: Leave empty or specify one or more 2-octet circuit numbers.

Function: Specifies inbound circuits.

Instructions: If you do not want this circuit to accept any inbound packets, leave the value for this parameter empty.

If you want this circuit to accept inbound packets, enter the circuit number or numbers, in 2-octet strings.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.20.1.11

Parameter: Out Circuits

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Static Forwarding Entries

Default: An empty list

Options: Leave empty or specify one or more outbound circuit number and time-to-live (TTL) threshold octet combinations.

Function: Specifies outbound circuits.

Instructions: If you do not want this circuit to forward any packets affected by this filter, leave the value for this parameter empty.

To define a circuit number and TTL threshold from which you want to forward packets, enter the octets as follows:

First 2 octets: circuit number

Next 2 octets: TTL threshold

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.20.1.12

Parameter: Forwarding Mode

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Static Forwarding Entries

Default: Static

Options: Static │ Static to Dynamic │ Dynamic to Static

Function: Specifies how this statically configured interface handles multicast packets.

Instructions: Choose Static if you want static forwarding of multicast packets without consulting multicast protocols or even without multicast protocols.

Choose Static to Dynamic if you want to accept multicast packets from a specified static configured nonmulticast interface and forward them to outbound interfaces running multicast protocols. If you choose this setting, you must also set the IGMP interface parameter Static Forward Cache Lifetime to a value appropriate for the multicast protocol.

Choose Dynamic to Static if you want to accept multicast packets from an interface running a multicast protocol and forward them on to static configured nonmulticast outbound interfaces.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.20.1.13

IGMP Boundary Group Parameters

Use the following descriptions to set IGMP boundary group parameters.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Admin Scope
Default: Enabled
Options: Enabled │ Disabled
Function: Specifies whether this record is enabled or disabled.
Instructions: To disable the boundary group record, enter Disabled.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.5.1.2

Parameter: Group Address

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Admin Scope
Default: None
Options: A valid group address
Function: Specifies the address of a multicast host group.
Instructions: Enter a group address to define this IGMP boundary record.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.5.1.3

Parameter: Prefix Length

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Admin Scope
Default: None
Options: A valid prefix for the group address
Function: Specifies a prefix for the multicast host group address.
Instructions: Enter an address prefix from 0 through 32 to define this IGMP boundary record.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.5.1.4

Parameter:	**Circuit List**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Admin Scope
Default:	None
Options:	A list of one or more circuit addresses
Function:	Specifies a list of circuit addresses for this boundary definition.
Instructions:	Specify each circuit with a 2-octet address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.5.1.5

Parameter:	**Tunnel List**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Admin Scope
Default:	None
Options:	A list of one or more multicast tunnels
Function:	Specifies a list of tunnels for this boundary address.
Instructions:	Specify each tunnel with an eight-octet address, four octets for the local IP address (the local end of the tunnel) and four octets for the remote IP address (the remote end of the tunnel).
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.5.1.6

Appendix B
Troubleshooting Commands

This appendix describes Bay Networks Technician Interface commands that you can use to troubleshoot a multicast network.

Topic	Page
mtrace Command	B-2
mrinfo Command	B-4
rsvp Command	B-5

mtrace Command

The **mtrace** command allows you to trace the branch of a multicast tree from a source to a receiver for a particular multicast group. Each branch of the tree is a data path consisting of multiple hops. The **mtrace** command displays statistics about packet rates and losses for each hop along the path.

To display statistical information, enter the **mtrace** command at the Technician Interface prompt as follows:

mtrace [*<options>*] *<source>* *<destination>* [*<group>*]

<options> = [**-e** *<extra_hops>* | **-g** *<gateway>* | **-i** *<if_addr>* | **-M** | **-m** *<max_hops>* | **-q** *<nqueries>* | **-r** *<resp_dest>* | **-s** | **-S** *<statint>* | **-t** *<ttl>* | **-U** | **-v** | **-w** *<wait>*]

Table B-1 describes each **mtrace** command option.

Table B-1. mtrace Options

Option	Meaning
-e *<extra_hops>*	Attempt to trace extra hops past a nonresponding router. The *extra_hops* value is an integer.
-g *<gateway>*	Send the trace query via a unicast packet directly to the multicast router *gateway* that you specify.
-i *<if_addr>*	Use *if_addr* as the local interface address for sending the trace query and as the default address for the receiver and the response destination. The value of *if_addr* is an IP address in dotted-decimal notation.
-M	Request the response using a multicast address.
-m *<max_hops>*	Set the maximum number of hops that are traced from the receiver back to the source to the integer you specify. The default *max_hops* value is 32.
-q *<nqueries>*	Set the maximum number of query attempts to the integer you specify. The default *nqueries* value is 3.
-r *<resp_dest>*	Send the trace response to a host (that is, the response destination) other than to the host on which **mtrace** is running, or to a multicast address other than the one registered for this purpose (224.0.1.32).
-s	Print a short-form report including only the multicast path, not the packet rate and loss statistics.

(continued)

Table B-1. mtrace Options *(continued)*

Option	Meaning
-S *<statint>*	Change the interval between statistics gathering traces to the specified number of seconds. The default value is 10 seconds.
-t *<ttl>*	Set the time to live (TTL) for multicast trace queries and responses to the value you specify. TTL equals the number of hops. The default *ttl* value is 127 hops. For local queries to the "all queries" multicast group, the default is one hop.
-U	Always request the response using unicast rather than attempting multicast first.
-v	Use verbose mode. In verbose mode, **mtrace** shows hop times on the initial trace and statistics display, as well as the route that was used to forward the initial trace.
-w *<wait>*	Set the time to wait for a trace response to the number of seconds you specify. The default *wait* value is 3 seconds.

source is the source of the multicast tree.

destination is the receiver for a particular multicast group.

group is a multicast group. The default group is 224.2.0.1. If you do not specify a group, the **mtrace** command does not display statistics.

For example, the following **mtrace** command specifies source 192.32.27.193, destination 192.32.199.162, and group 224.2.0.1.

```
$ mtrace 192.32.27.193 192.32.199.162 224.2.0.1
Mtrace from 192.32.27.193 to 192.32.199.162 via group 224.2.0.1
Querying full reverse path...
  0  192.32.199.162
 -1  192.32.199.162  DVMRP  thresh^ 1
 -2  192.32.27.193
Round trip time 1039 ms; total ttl of 2 required.
Waiting to accumulate statistics...
  Source        Response Dest    Overall     Packet Statistics For
Traffic From
192.32.27.193   192.32.199.161   Packet      192.32.27.193 To
224.2.0.1
     v       __/  rtt    3ms     Rate        Lost/Sent = Pct  Rate
192.32.27.193
192.32.199.162
     v      \__   ttl    2         0 pps
192.32.199.162     * * *
  Receiver      Query Source
```

mrinfo Command

The **mrinfo** command displays the capabilities of a DVMRP multicast router. It shows whether the router supports **mtrace** and pruning, provides revision information, and provides the link characteristics for every link on the router.

To display this information, enter the **mrinfo** command at the Technician Interface prompt as follows:

mrinfo [*<options>*] *<router_address>*

<options> = [**-r** *<retry_count>* | **-t** *<timeout_count>*]

Table B-2 describes each **mrinfo** command option.

Table B-2. mrinfo Options

Option	Meaning
-r *<retry_count>*	Set the neighbor query retry limit to *retry_count*. The default is three retries.
-t *<timeout_count>*	Set the number of seconds to wait for the neighbor query reply to *timeout_count*. The default timeout is 3 seconds.

router_address is the address of the DVMRP router whose capabilities you want to display.

For example, the following **mrinfo** command displays the capabilities of DVMRP router 192.32.27.46. The DVMRP router is running Version 3.255 and supports pruning and **mtrace**.

```
$ mrinfo 192.32.27.46
192.32.27.46 [version 3.255,prune,genid,mtrace]:
  192.32.27.46 -> 192.32.27.39 [1/1]
  192.32.27.46 -> 192.32.27.47 [1/1]
  192.32.27.46 -> 192.32.191.2 [1/1/tunnel]
  192.32.27.161 -> 192.32.27.162 [1/1]
```

rsvp Command

The **rsvp** command allows you to view information about RSVP and set global configuration parameters.

Enter the **rsvp** command at the Technician Interface prompt as follows:

rsvp *<subcommand>* [*<options>*]

<subcommand> = {**session** | **phop** | **oi** | **path** | **resv** | **blockade**}

Table B-3 describes each **rsvp** subcommand.

Table B-3. rsvp Subcommands

Subcommand	System Displays
session	Known RSVP sessions
phop	Known RSVP previous hops
oi	Known RSVP outgoing interfaces
path	RSVP path state
resv	RSVP RESV state
blockade	RSVP blockade state

<options> = [**-d** *<destination_IP>* [*<protocol_ID>* | *<destination_port>*] | **-p** *<previous_hop>* | **-f** *<source_IP>* [*<source_port>*] | **-n** *<next_hop>*]

The options apply to subcommands, as described in Table B-4.

Table B-4. Options for rsvp Subcommands

Option	Effect	Applicable Subcommands
-d *<destination_IP>* [*<protocol_ID>* | *<destination_port>*]	Retrieves RSVP data for the session you specify	session, phop, oi, path, resv
-p *<previous_hop>*	Retrieves only sessions with the specified previous hop	phop, path, resv
-f *<source_IP>* [*<source_port>*]	Retrieves only oi, path, or resv information for sessions with a source address of *source_IP* and, optionally, a source port of *source_port*	oi, path, resv
-n *<next_hop>*	Retrieves only reservation request information with the specified next hop	resv

For example, the following **rsvp** command specifies the RSVP previous hops:

$ **rsvp phop**

```
RSVP Previous Hops:

      Session
IP dest/protocol/dest port   Previous Hop
--------------------------   ---------------
225.1.1.1 17 5000            199.1.4.5
225.1.1.1 17 5000            200.1.1.212
225.1.1.1 17 5000            201.1.1.212

   3 previous hops matched
```

Index

A

accept DVMRP route policies. *See* MOSPF

accept policies
- DVMRP, 4-74
- DVMRP unicast, 4-69
- MOSPF accept DVMRP route, 5-11

acronyms, xxi

Action parameter
- DVMRP
  - accept policies, 4-77, A-65
  - announce policies, 4-82, A-70
  - unicast accept policies, 4-72, A-60
- IGMP group policies, 3-32, A-77
- MOSPF accept DVMRP route policies, 5-11, A-73

addresses, multicast, 1-3

Advertise Aggregate parameter (DVMRP announce policies), 4-82, A-71

Advertise Self parameter (DVMRP interface), 4-43, A-10

announce policies, DVMRP, 4-79

ASBR (autonomous system boundary router) in multicasting, 5-2

assert messages (PIM), 6-7

B

Bandwidth Interval (Secs) parameter (Line Resource Manager), 8-8, A-30

border router (BR) in multicasting, 5-2

boundary router (ASBR) in multicasting, 5-2

C

Cache Time Out parameter (PIM interface), 6-33, A-52

Candidate BSR Hash Mask Length parameter (PIM global), 6-25, A-43

Candidate BSR Interval parameter (PIM global, 6-25, A-42

Candidate BSR IP Address parameter (PIM global), 6-25, A-42

Candidate BSR parameter (PIM global), 6-25, A-41

Candidate BSR Priority parameter (PIM global), 6-25, A-42

Candidate RP Advertise Interval parameter (PIM global), 6-26, A-45

Candidate RP Group/Mask parameter (PIM global), 6-26, A-45

Candidate RP IP Address parameter (PIM global), 6-26, A-44

Candidate RP parameter (PIM global), 6-26, A-43

Candidate RP Priority parameter (PIM global), 6-26, A-44

Candidate RP Register Cache Timeout parameter (PIM global), 6-26, A-46

Circuit List parameter (IGMP boundary group), 3-30, A-85

Circuit Name parameter (IGMP static host), 3-29, A-22

Cisco Compatible parameter (PIM global), 6-29, A-47

Control Message Mode parameter (DVMRP tunnel), 4-65, A-14

conventions, text, xx

cost of a route, defined, 4-10

customer support, xxiv

D

dataflow, defined, 1-4

Debug Level parameter (DVMRP global), 4-29, A-6

Debug Log Filter parameter (RSVP global), 7-6, A-55

debug messages, logging
- DVMRP, 4-29
- IGMP, 3-10
- PIM, 6-30
- RSVP, 7-6

Debug parameter
- IGMP global, 3-11, A-19
- PIM global, 6-30, A-49

Default Join/Prune Interval parameter (PIM global), 6-24, A-40

default route, DVMRP circuit
- advertising, 4-44
- generating, 4-44
- listening for, 4-46

default route, DVMRP tunnel
- advertising, 4-62
- generating, 4-62
- listening for, 4-64

deleting protocols from an interface
- DVMRP, 4-84
- IGMP, 3-39
- PIM, 6-37
- RSVP, 7-14

Designated Router Timeout parameter (IGMP interface), 3-23, A-24

directly connected neighbors (DVMRP), defined, 4-2

disabling
- DVMRP
  - accept policies, 4-78
  - announce policies, 4-83
  - globally, 4-9
  - on a circuit, 4-31
  - on a tunnel, 4-53
  - unicast accept policies, 4-73
- IGMP
  - boundary group, 3-31
  - globally, 3-5
  - group policies, 3-33
  - on an interface, 3-16
  - static forwarding policies, 3-38

disabling *(continued)*
- MOSPF
  - accept DVMRP route policies, 5-12
  - globally, 5-4
- PIM
  - globally, 6-20
  - on an interface, 6-31
- RSVP on an interface, 7-7

Distance Vector Multicast Routing Protocol. *See* DVMRP

Downstream IGMP Relay parameter (PIM interface), 6-35, A-53

DVMRP (Distance Vector Multicast Routing Protocol)
- accept policies, 4-74
- announce policies, 4-79
- cost
  - of a route, defined, 4-10
  - of a tunnel, 4-56
  - of an interface, 4-35
- default route, advertising
  - on a tunnel, 4-62
  - on an interface, 4-44
- default route, listening for
  - on a tunnel, 4-64
  - on an interface, 4-46
- deleting from an interface, 4-84
- disabling
  - globally, 4-9
  - on a circuit, 4-31
- enabling
  - globally, 4-9
  - on a circuit, 4-31
- encapsulation mode, 4-54
- forwarding table size, 4-39
- IGMP Relay device, configuring router for use with, 9-20
- local networks, advertising, 4-42
- logging messages, 4-29
- messages, logging event, 4-29
- neighbor routers
  - accepting reports from, via circuit, 4-47
  - accepting reports from, via tunnel, 4-66
- policies
  - accept, 4-74
  - announce, 4-79
  - unicast accept, 4-69
- probe interval, 4-21

DVMRP (Distance Vector Multicast Routing Protocol) (*continued*)
reports from DVMRP neighbors
via circuit, 4-47
via tunnel, 4-66
route costs
defined, 4-10
interface, 4-35
tunnel, 4-56
route switch interval, 4-23
router capabilities, displaying, B-4
routes
estimating number of, 4-25
how DVMRP chooses, 4-5
specifying maximum number of, 4-27
shortest path tree, 4-6
starting, 2-4
tree pruning, 4-7
tunnel addresses, 4-51
tunnel, threshold value of a, 4-57
unicast accept policies, 4-69
DVMRP Networks parameter (MOSPF accept DVMRP route policies), 5-11, A-74

E

Enable parameter
DVMRP
accept policies, 4-78, A-64
announce policies, 4-83, A-69
circuit, 4-31, A-7
global, 4-9, A-2
tunnel, 4-53, A-12
unicast accept policies, 4-73, A-59
IGMP
boundary group, 3-31, A-84
global, 3-5, A-17
group policies, 3-33, A-76
interface, 3-17, A-22
static forwarding policies, 3-38, A-80
MOSPF accept DVMRP route policies, 5-12, A-73
PIM
global, 6-20, A-37
interface, 6-31, A-51
RSVP
global, 7-4, A-54
interface, 7-7, A-56
enabling
DVMRP
globally, 4-9
on a circuit, 4-31
on a tunnel, 4-53
IGMP
boundary group, 3-31
globally, 3-5
group policies, 3-33
on an interface, 3-16
static forwarding policies, 3-38
MOSPF
accept DVMRP route policies, 5-12
globally, 5-4
PIM
globally, 6-20
on an interface, 6-31
RSVP on an interface, 7-7
Encapsulation Mode parameter (DVMRP tunnel), 4-55, A-12
Estimated Bandwidth parameter (line resources), 2-11, 8-4, A-28
Estimated Groups parameter (IGMP global), 3-7, A-17
Estimated Routes parameter (DVMRP global), 4-26, A-5
event messages, logging
DVMRP, 4-29
IGMP, 3-10
PIM, 6-30
RSVP, 7-6

F

first fit multiline select algorithm (line resources), 8-12
Forward Cache Limit parameter, 3-13, A-18
Forward Cache Size parameter
DVMRP circuit, 4-40, A-9
DVMRP tunnel, 4-60, A-13
Forward Cache TTL parameter
DVMRP circuit, 4-41, A-9
DVMRP tunnel, 4-61, A-13
Forwarding Mode parameter (IGMP static forwarding policies), 3-37, A-83

forwarding table (DVMRP), defined, 4-39
Full Update Interval parameter (DVMRP global), 4-11, A-3

G

Garbage Timeout parameter (DVMRP global), 4-16, A-5
Generate Neighbor Hello ID parameter (PIM global), 6-24, A-41
Group Address parameter
  IGMP boundary group, 3-30, A-84
  IGMP static group, 3-29, A-21
Groups parameter
  IGMP group policies, 3-32, A-78
  IGMP static forwarding policies, 3-37, A-81
groups, multicast host, 1-2

H

Hello Interval parameter (PIM interface), 6-32, A-51
host groups
  membership reports (IGMP), 3-2
  types, 1-2

I

IGMP (Internet Group Management Protocol)
  boundary group
    configuring, 3-30
    disabling, 3-31
    enabling, 3-31
  cache entry for mtrace, lifetime of, 3-26
  deleting from an interface, 3-39
  designated router timeout interval, 3-22
  disabling
    globally, 3-5
    on an interface, 3-16
  enabling
    globally, 3-5
    on an interface, 3-16
  function of, 3-2
  group membership, timeout interval, 3-21
IGMP (Internet Group Management Protocol) *(continued)*
  group policies
    configuring, 3-32
    disabling, 3-33
    enabling, 3-33
  groups, estimating number of, 3-6
  host leave messages, 3-3
  host membership
    queries, 3-2
    reports, 3-3
  host response time, maximum, 3-24
  lifetime of a cache entry for mtrace, 3-26
  logging messages, 3-10
  messages
    host leave, 3-3
    logging event, 3-10
  mtrace, lifetime of a cache entry for, 3-26
  policies
    group, 3-32
    static forwarding, 3-33
  query rate, 3-19
  starting, 2-2
  static forwarding policies
    configuring, 3-33
    disabling, 3-38
    enabling, 3-38
  static host entry, 3-28
  timeout interval
    for designated router, 3-22
    for group membership, 3-21
  version threshold time, 3-8
IGMP (Internet Group Management Protocol) Relay
  backup configurations, 9-22
  configuring, 9-1
  data forwarding, upstream, 9-12
  disabling globally, 9-9
  downstream hosts, 9-3
  DVMRP router with, 9-20
  enabling globally, 9-9
  hosts, downstream, 9-3
  how it works, 9-4
  interface type, 9-13
  MOSPF boundary router with, 9-18
  overview, 9-2

IGMP (Internet Group Management Protocol) Relay *(continued)*
reports, unsolicited, 9-16
router redundancy, 9-23
timeout values for multicast table entries, 9-11
topology, 9-3
type of interface, 9-13
unsolicited reports, 9-16
upstream
data forwarding, 9-12
multicast routers, 9-3
In Circuits parameter (IGMP static forwarding policies), 3-37, A-82
Incoming Gateways parameter (DVMRP accept policies), 4-77, A-67
Incoming Networks parameter, DVMRP
accept policies, 4-77, A-65
announce policies, 4-82, A-69
unicast accept policies, 4-72, A-60
Inflate Reservations Percentage parameter (RSVP), 8-9, A-31
Info Log Filter parameter (RSVP global), 7-6, A-55
Info/Warnings parameter (PIM global), 6-30, A-48
Inject Aggregate parameter
DVMRP accept policies, 4-77, A-66
DVMRP unicast accept policies, 4-72, A-62
Inject List parameter (MOSPF accept DVMRP route policies), 5-11, A-75
Interface Membership Timeout parameter (IGMP interface), 3-21, A-23
Interface Query Rate parameter (IGMP interface), 3-20, A-23
internal router (IR) in multicasting, 5-2
Internet Group Management Protocol. *See* IGMP
IP Address parameter (IP configuration), A-26

J

Join Ack Enable parameter (IGMP global), 3-12, A-18
Join/Prune Interval parameter (PIM interface), 6-34, A-53
join/prune messages (PIM), 6-7

L

Largest Bandwidth parameter (line resources), 8-15, A-34
Largest Buffer parameter (line resources), 8-16, A-34
Last Hop Data Threshold parameter (PIM global), 6-21, A-38
Last Hop Threshold parameter (PIM global), 6-21, A-38
Leaf Timeout parameter (DVMRP global), 4-20, A-3
leaky bucket policing algorithm (line resources), 8-10
Line Resource Manager (LRM)
bandwidth interval, 8-8
latency for reserved flow packet, 8-14
multiline select algorithms, 8-12
multiline threshold bandwidth, 8-13
overview, 8-2
policing algorithm, 8-7, 8-10
reservations, inflate by percentage, 8-9
traffic queuing algorithm, 8-6
unreserved packets in queue, specifying maximum, 8-11
Listen Default Route parameter (DVMRP circuit), 4-46, A-10
Local DR Priority parameter (PIM interface), 6-36, A-54
Local IP Address parameter (DVMRP tunnel), 4-52, A-16
logging messages
DVMRP, 4-29
IGMP, 3-10
PIM, 6-30
RSVP, 7-6
LSSR option, 4-54

M

Max Host Response Time parameter (IGMP interface), 3-25, A-24
Max Routes parameter (DVMRP global), 4-28, A-7

messages, logging
DVMRP, 4-29
IGMP, 3-10
PIM, 6-30
RSVP, 7-6
Metric parameter, DVMRP
accept policies, 4-77, A-68
announce policies, 4-82, A-72
circuit, 4-36, A-8
tunnel, 4-56, A-12
unicast accept policies, 4-72, A-63
metric, route, 4-5
MOSPF (Multicast OSPF)
accept DVMRP route policies, 5-11
configuring for IGMP Relay device, 9-18
disabling globally, 5-4
enabling globally, 5-4
forwarding timeout value, 5-5
multicasting support, types of, 5-3
overview, 5-1
starting, 2-6
timeout value, 5-5
mrinfo command, B-4
mtrace command, 3-26, B-2
Mtrace Entry Lifetime parameter (IGMP interface), 3-27, A-24
Multicast Downstream IGMP Relay parameter (OSPF/MOSPF global), 5-10, A-36
Multicast Dynamic TTL parameter (OSPF/MOSPF global), 5-7, A-36
Multicast Extensions parameter (OSPF/MOSPF global), 2-6, 5-4, A-35
Multicast Forwarding parameter (OSPF/MOSPF global), 5-9, A-37
Multicast Max Queued Pkts parameter (OSPF/MOSPF global), 5-6, A-35
multicast migration tools, 1-6
Multicast OSPF. *See* MOSPF
Multicast Table Manager, 1-5
Multicast Timeout Value parameter (OSPF/MOSPF global), 5-5, A-35
multicasting
addresses for, 1-3
BCC show commands for, 1-13
border router (BR), 5-2
boundary router (ASBR), 5-2
capabilities of DVMRP router, displaying, B-4
commands
mrinfo, B-4
mtrace, B-2
rsvp, B-5
comparing routes (DVMRP), 4-6
creating a shortest-path tree (DVMRP), 4-6
definition of, 1-2
host groups, 1-2
internal router (IR), 5-2
leaf network (DVMRP), 4-7
migration, 1-6
Multicast Table Manager, 1-5
threshold, 4-37
trace branch from source to receiver for multicast group, B-2
tunnel (DVMRP), 4-2
types supported by MOSPF, 5-3
Multiline Select Algorithm parameter (line resources), 8-12, A-32
Multiline Threshold Bandwidth parameter (line resources), 8-13, A-33

N

Name parameter
DVMRP
accept policies, 4-77, A-64
announce policies, 4-82, A-69
unicast accept policies, 4-72, A-59
IGMP
group policies, 3-32, A-76
static forwarding policies, 3-37, A-80
MOSPF accept DVMRP route policies, 5-11, A-73
Neighbor Probe Interval parameter (DVMRP global), 4-22, A-6
Neighbor Timeout parameter (DVMRP global), 4-18, A-4

neighbors, DVMRP
communicating with other routers
via circuit, 4-47
via tunnel, 4-66
directly connected, defined, 4-2
tunnel-connected, defined, 4-2
Nonlocal Reports parameter (IGMP global), 3-14, A-20

O

Out Circuits parameter (IGMP static forwarding policies), 3-37, A-83
Outgoing Interfaces parameter (DVMRP announce policies), 4-82, A-71
Outgoing Tunnels parameter (DVMRP announce policies), 4-82, A-72

P

permanent host group, 1-2
PIM (Protocol Independent Multicast)
bootstrap router, 6-5
cache timeout interval, 6-33
candidate bootstrap routers, 6-5
candidate BSR configuration, 6-25
candidate RP routers, 6-4, 6-26
Cisco router compatibility, 6-29
configuration prerequisites, 2-7
deleting from an interface, 6-37
designated router, defined, 6-3
disabling
globally, 6-20
on an interface, 6-31
enabling
globally, 6-20
on an interface, 6-31
Hello interval, 6-32
hosts, 6-3
IGMP Relay on downstream device, 6-35
join/prune interval
for an interface, 6-34
global default, 6-23
last-hop router, 6-3
last-hop threshold configuration, 6-20
local DR priority, 6-36
logging messages, 6-30
PIM (Protocol Independent Multicast) *continued*
messages
assert, 6-7
join/prune, 6-7
logging event, 6-30
neighbor Hello ID, 6-24
register, 6-7
neighbor Hello ID messages, 6-24
network components, 6-3
probe timer, 6-28
receiver
joining multicast group, 6-10
leaving multicast group, 6-12
register suppression timer, 6-27
rendezvous point threshold, 6-21
rendezvous point, defined, 6-4
router compatibility, Cisco, 6-29
shared tree, defined, 6-8
shortest-path tree
defined, 6-8
last-hop router, 6-17
RP router, 6-15
starting, 2-8
threshold sample interval, 6-22
timeout interval, cache, 6-33
timers
probe, 6-28
register suppression, 6-27
policies
DVMRP
accept, 4-74
announce, 4-79
unicast accept, 4-69
IGMP
group, 3-32
static forwarding, 3-33
MOSPF accept DVMRP route policies, 5-11
Policing Algorithm parameter (line resources), 8-7, A-30
Prefix Length parameter
IGMP boundary group, 3-30, A-84
IGMP static host, 3-29, A-21
priority queuing limits (line resources), 8-11, A-32
Probe Time parameter (PIM global), 6-28, A-47
product support, xxiv
Protocol Independent Multicast. *See* PIM

Prune Life Time parameter, DVMRP
circuit, 4-49, A-11
tunnel, 4-68, A-15
Pruning Enable parameter (DVMRP global), 4-12, A-7
pruning the shortest-path tree (DVMRP), 4-7
publications
Bay Networks, xxiii
related, xxiii

Q

quality of service (QoS), 8-2
Query Suppression parameter (IGMP interface), 3-18, A-25
queue limit policing algorithm (line resources), 8-10
queuing, priority limits (line resources), 8-11

R

Received on Interfaces parameter
DVMRP accept policies, 4-77, A-67
DVMRP unicast accept policies, 4-72, A-62
Received on Tunnels parameter (DVMRP accept policies), 4-77, A-68
Receivers parameter (IGMP group policies), 3-32, A-79
Receivers' Circuits parameter (IGMP group policies), 3-32, A-79
Refresh Blockade Multiple parameter (RSVP circuit), 7-10, A-56
Refresh Interval parameter (RSVP circuit), 7-8, A-57
Refresh Multiple parameter (RSVP circuit), 7-9, A-57
register messages (PIM), 6-7
Register Suppression Timer parameter (PIM global), 6-27, A-46
register-stop messages (PIM), 6-7
Relay Circuit Type parameter (IGMP Relay interface), 9-15, A-26
Relay Forwarding Timeout parameter (IGMP Relay global), 9-11, A-20
Relay parameter (IGMP Relay global), 9-10, A-19
Relay Report Interval parameter (IGMP Relay interface), 9-17, A-26
Relay Upstream Forwarding parameter (IGMP Relay global), 9-13, A-20
Remote IP Address parameter (DVMRP tunnel), 4-52, A-16
Rendezvous Point (RP) Threshold parameter (PIM global), 6-22, A-39
Report Depend Probe parameter
DVMRP circuit, 4-48, A-11
DVMRP tunnel, 4-67, A-15
Reservable Bandwidth parameter (line resources), 2-11, 8-5, A-29
Reservation Latency parameter (line resources), 8-14, A-33
Resource Manager, 1-5, 8-3
Resource Reservation Protocol. *See* RSVP
RFC 1075, 4-54
round robin multiline select algorithm (line resources), 8-12
route costs (DVMRP)
defined, 4-10
interface, 4-35
tunnel, 4-56
Route Delay parameter (RSVP circuit), 7-12, A-58
Route Enable parameter (DVMRP circuit), 4-34, A-8
Route Expiration Timeout parameter (DVMRP global), 4-14, A-4
Route Listen parameter (DVMRP tunnel), 4-64, A-14
route metric, defined, 4-5
Route Preference parameter (DVMRP unicast accept policies), 4-72, A-61
Route Supply parameter (DVMRP tunnel), 4-63, A-14
Route Switch Timeout parameter (DVMRP global), 4-24, A-6
Route Type parameter (DVMRP unicast accept policies), 4-72, A-63
RP Data Threshold parameter (PIM global), 6-22, A-39

RSVP (Resource Reservation Protocol)
bandwidth
estimated, 8-4
reservable, 8-5
deleting from an interface, 7-14
disabling, 7-7
displaying information using Technician Interface, B-5
enabling, 7-7
estimated bandwidth, 8-4
lifetime multiplier, 7-9
logging messages, 7-6
messages, logging event, 7-6
multiplier
lifetime, 7-9
refresh blockade, 7-10
overview, 7-1
refresh blockade multiplier, 7-10
refresh timer, 7-8
reservable bandwidth, 8-5
route delay value, 7-12
rsvp command, B-5
setting parameters using Technician Interface, B-5
slot, configuring on, 7-5
starting, 2-10
TTL override, 7-11
UDP encapsulation, 7-13
rsvp command, B-5
RSVP TTL parameter (RSVP circuit), 7-11, A-57
Rule Precedence parameter
DVMRP
accept policies, 4-77, A-66
announce policies, 4-82, A-70
unicast accept policies, 4-72, A-61
IGMP
group policies, 3-32, A-78
static forwarding policies, 3-37, A-81
MOSPF accept DVMRP route policies, 5-11, A-74

S

show commands, 1-13
Soloist Slots parameter (RSVP global), 7-5, A-55
source network (DVMRP), defined, 4-4
Sources parameter
IGMP group policies, 3-32, A-77
IGMP static forwarding policies, 3-37, A-82
starting
DVMRP, 2-4
IGMP, 2-2
MOSPF, 2-6
PIM, 2-8
RSVP, 2-10
Static Forward Cache Lifetime parameter (IGMP interface), 3-28, A-25
Subnet Mask parameter (IP configuration), A-27
Supply Default Route parameter (DVMRP circuit), 4-45, A-10
support, Bay Networks, xxiv

T

technical publications, xxiii
technical support, xxiv
text conventions, xx
Threshold parameter
DVMRP circuit, 4-38, A-9
DVMRP tunnel, 4-58, A-13
Threshold Sample Interval parameter (PIM global), 6-23, A-40
threshold values (DVMRP), function, 4-37
timers
designated router timeout (IGMP), 3-22
garbage timeout (DVMRP), 4-16
group membership timeout (IGMP), 3-21
leaf (DVMRP), 4-19
multicast timeout (MOSPF), 5-5
neighbor report (DVMRP), 4-17
probe (PIM), 6-28
refresh interval (RSVP), 7-8
register suppression (PIM), 6-27
route expiration (DVMRP), 4-13
unconfirmed route timeout (DVMRP), 4-15
Trace Log Filter parameter (RSVP global), 7-6, A-56
Trace parameter (PIM global), 6-30, A-50
traffic filters, effect on multicast data packets, 1-2
Traffic Queuing Algorithm parameter (line resources), 8-6, A-29

transient host group, 1-2
Transmit Bcast Addr parameter (IP configuration), A-27
tree pruning (DVMRP), 4-7
trees
  shared (PIM), 6-8
  shortest-path (DVMRP), 4-6
  shortest-path (PIM), 6-8
Triggered Update Interval parameter (DVMRP global), 4-11, A-3
triggered updates, 4-10
Tunnel List parameter (IGMP boundary group), 3-30, A-85
tunnel-connected neighbors (DVMRP), defined, 4-2
tunnels (DVMRP)
  addresses for, 4-51
  configuring, 4-50
  cost, 4-56
  disabling, 4-53
  enabling, 4-53
  forwarding table for, 4-59
  neighbor connections, 4-2
  threshold value for, 4-57
  unicast, disabling multicast support on, 4-33

U

UDP encapsulation (RSVP circuit), 7-13
Udp Required parameter (RSVP circuit), 7-13, A-58
UnNumbered Assoc Address parameter (IP configuration), A-28
Unreserved Policing Algorithm parameter (line resources), 8-10, A-31
Unreserved Queue Length parameter (line resources), 8-11, A-32
update interval (DVMRP), 4-10
Use Global Join/Prune Interval parameter (PIM interface), 6-34, A-52

V

Version Threshold Time parameter (IGMP global), 3-9, A-18